МЕТОДИКА НАВЧАННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Co-funded by the
Erasmus+ Programme
of the European Union

Академічна протидія гібридним загрозам
Проєкт програми ЄС Еразмус+
№ 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP

«Академічна протидія гібридним загрозам»
№ 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP

МЕТОДИКА НАВЧАННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Посібник

Харків, 2023

УДК 378.147:351.861
М 54

Автори:
Едуард Балашов, Михайло Білоконь, Тетяна Борозенцева, Марія Головянко, Світлана Гришко, Тарас Жовтенко, Оксана Карпенко, Ольга Копієвська, Олександр Котуков, Павло Худ

М 54 Методика навчання в умовах гібридних загроз: посібник / Е. Балашов, М. Білоконь, Т. Борозенцева, М. Головянко, С. Гришко, Т. Жовтенко та ін. – Харків: ТОВ "ТЕХНОЛОГІЧНИЙ ЦЕНТР ГРУП", 2023. – 84 с.

DOI: 10.62067/978-617-8242-02-2
ISBN 978-617-8242-02-2 (on-line)

Посібник з методики навчання в умовах гібридних загроз створений як один із результатів проєкту WARN "Академічна протидія гібридним загрозам", за фінансової підтримки програми ЄС Еразмус+, №610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP. Мета проєкту полягає у підвищенні рівня національної безпеки шляхом подолання нестачі суспільних безпекових сервісів, яка виникла через появу гібридних загроз. Це – загрози нового типу, вони створюються скоординованими та синхронізованими діями, які свідомо спрямовані на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів. Головною вразливістю гібридних загроз стає демократичний процес прийняття рішень та всі, хто бере в ньому участь. Люди опиняються незахищеними, якщо не вміють розпізнавати гібридні загрози, визначати не локальну, а загальну мету гібридних впливів, а також – об'єднувати зусилля та захищати свій робочий та соціальний простір від гібридних загроз. Для ефективної протидії цьому новому типу загроз проєкт WARN запровадив превентивне навчання та підготовку громадян як агентів захисту. Це стає можливим завдяки додаванню до будь-якої освітньої програми унікальної компетентності, що спрямована на вміння виконувати свої професійні та громадські обов'язки в неочікуваних, непрогнозованих, навіть – в екстремальних ситуаціях, спричинених гібридними загрозами. Специфічна методика навчання є невід'ємною складовою формування такої компетентності, бо саме вона дозволяє напрацьовувати навички комплексного захисту та протидії гібридним загрозам.

УДК 378.147:351.861
ISBN 978-617-8242-02-2 (on-line)

Цей проект був профінансований за підтримки Європейської Комісії.
Ця публікація відображає лише погляди автора, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься в ній.

ЗМІСТ

СПИСОК ТАБЛИЦЬ

СПИСОК РИСУНКІВ

ВСТУП

Тарас Жовтенко[1]
Едуард Балашов[1]
[1]Національний університет "Острозька академія"

Формування безпекової політики України відбувається в умовах активного протистояння сучасним безпековим викликам, новим та унікальним не лише для нашої держави, але й для світу загалом.

На ці виклики нашаровуються динамічні процеси сучасних геополітичних змін у регіоні та світі, які характеризуються закінченням глобальної конфронтації, викликаної ідеологічним протиборством двох світових систем. Разом з тим, сьогодні залишаються протиріччя, що пов’язані з розбіжностями національних інтересів, цілей, позицій України на внутрішньому, регіональному та світовому рівнях.

Викликають занепокоєння такі негативні чинники, як поляризація рівня життя, деградація навколишнього середовища, розповсюдження загрозливих хвороб, виникнення невідомих раніше масових захворювань, неконтрольована міграція, етнічні та конфесійні напруження, збільшення масштабів і частоти техногенних катастроф. Вони призводять до пересування центру традиційних загроз (збройне вторгнення) у бік нетрадиційних, зростання яких значною мірою зумовлено інформаційною відкритістю сучасного суспільства, вразливістю великих індустріальних міст.

Ці процеси лежать в основі тренду "гібридизації" сучасних загроз національній та міжнародній безпеці.

Гібридне протистояння України та російської федерації, яке почалося з військово-політичної та інформаційної агресії Кремля на початку 2014 року, практично від самого свого початку поставило під сумнів майже усі засади сформованої системи міжнародної

безпеки. Відтак, для України та країн Західного світу актуальним є пошук адекватної та ефективної системи реагування на виклики та загрози, які принесли з собою ці події.

Відмітною рисою гібридного інструментарію є використання широкого спектру інструментів – від воєнної сили (регулярних сил та нерегулярних збройних формувань) до активного інформаційно-психологічного впливу в ключових сферах інформаційної інфраструктури противника (дезінформація, пропаганда в традиційних медіа та соціальних мережах, кібератаки, активні заходи спецслужб тощо), використання інструментів політичного, економічного, гуманітарного впливу.

Гібридна агресія характеризується мультидоменністю, одночасним використанням різноманітних комбінацій інструментарію, які варіюються залежно від динаміки гібридного конфлікту, реакції противника та змін безпекового середовища на регіональному та глобальному рівнях.

Для протидії такій комплексній і динамічній загрозі вкрай необхідні нові підходи до розуміння та формування архітектури не лише систем національної безпеки окремих держав. Необхідною умовою ефективної протидії гібридному інструментарію є створення динамічного, комплексного середовища забезпечення безпеки, побудованого у відповідності до логіки самої гібридної загрози – на спільних засадах універсальності та мультидоменності.

Формування такого середовища – не лише сфера відповідальності національних урядів окремих держав та їх секторів безпеки та оборони. Для ефективної протидії гібридним інструментам та створення надійної системи захисту необхідно залучати усі домени-потенційні об’єкти гібридних атак, а також створити надійну систему синергії між академічною і практичною сферами суспільства і держави.

Запорукою цього є формування універсальної і сучасної системи науково-практичного розуміння природи та сутності гібридної загрози та її складових.

Існування такої системи неможливе без розробки новітньої методики для широкого кола академічної спільноти та фахівців-практиків з вивчення, виявлення, аналізу та протидії сучасним гібридним загрозам.

Така інноваційна методика "гібридного навчання" має базуватися на основі:

– проактивного захисту: фокусується на виявленні потенційних загроз;

– змагальних моделей навчання (на основі сучасного штучного інтелекту);

– предметно-орієнтованих ігор;

– інтелектуальної технології моделювання сценаріїв гібридних загроз, специфічних для реалій України.

Пропонований посібник фокусується на плануванні та проведенні лекційних та практичних занять відповідно до нових методик, проведення тематичних воркшопів, майстер-класів, використанні технологій бренйшторму та симуляцій, змагальних ігор та інтелектуальних спарингів.

Подяка

Ми вдячні експертам з Університету м. Ювяскюля (Фінляндія) – проф. О. Кайковій та проф. В. Терзіяну за неординарні ідеї, унікальну співпрацю, організаційні та дослідницькі можливості, надані нашій команді, – всього того, що спрямовувало та надихало при створенні цього посібника.

Також ми вдячні експертам дослідницької організації TNO (Нідерланди), завдяки яким ми не лише познайомились із світом навчальних ігор, але й отримали можливість занурились в їх дивовижну атмосферу.

1. ОСВІТА ЯК ЗАХИСТ ВІД ГІБРИДНИХ ЗАГРОЗ

Світлана Гришко[1]
Марія Головянко[1]
[1]Харківський національний університет радіоелектроніки

1.1. Розуміємо небезпеку: на що потрібно звернути увагу

Навчання завжди відігравало важливу роль для розвитку людства та підтримки його життєздатності:

– навчання дає людям знання та навички, які потрібні для праці та життя;

– навчання допомагає розвивати мислення та креативність, виховує здатність аналізувати інформацію, ставити питання, шукати відповіді, розв›язувати проблеми;

– навчання допомагає людям розуміти інших людей та розвивати толерантність та розуміння різних культур та світоглядів.

Ці фундаментальні задачі освітнього процесу зберігають свою актуальність і сьогодні. Але змінюються умови їх реалізації: по-перше, змінюються умови самого процесу навчання; по-друге, змінюються умови життя, до яких викладачі готують своїх учнів. Серед таких змін – поява гібридних загроз. Особливістю ситуації є те, що професійний безпековий сектор не має достатніх можливостей та ресурсів для самостійної протидії складним гібридним загрозам. Він потребує можливості спиратись на обізнаність суспільства про гібридні загрози та способи захисту в таких умовах. Це визнається низкою офіційних документів, наприклад:

– спільна рамка ЄС та НАТО з протидії гібридним загрозам вказує, що підвищення обізнаності громадськості про гібридні загрози

є одним основних факторів розвитку соціальної стійкості (*European Council, European Commission, NATO, 2016; п. 3.2*);

– в огляді НАТО відзначається: для протидії гібридним загрозам "важливість освіченої громадськості не можливо перебільшити" (*Hagelstam, 2018*);

– План дій цифрової освіти ЄС розглядає освіту як один з інструментів стійкості суспільства та протидії сучасним викликам (*European Council, European Commission, European Economic and Social Committee, 2020*);

– в огляді НАТО, який охоплює заходи з протидії гібридним загрозам (*NATO, 2023*), підкреслюється важлива роль тренувань, навчання, освіти та співпраці військових та невійськових учасників;

– фінська концепція комплексної безпеки, яка вважається однією з найефективніших в умовах гібридних загроз, базується на підготовленості всього суспільства до несподіваних викликів, включно із стійкістю домогосподарств (концепція "72 години") та обізнаністю суспільства, зокрема – завдяки національним курсам оборони (*Turvallisuuskomitea, 2017*).

Таким чином, навчання, освіта та загальна обізнаність суспільства відіграють одну з ключових ролей для протидії гібридним загрозам. Вони мають закрити нестачу навичок у людей, які приймають рішення щодо розпізнавання гібридних загроз, визначення їх мети, прогнозування наслідків власних дій при гібридних впливах та захисту свого робочого і соціального простору від гібридних загроз.

В рамках роботи над проєктом Еразмус+ "Академічна протидія гібридним загрозам" (**WARN**) 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP була сформульована ключова компетентність, необхідна для забезпечення безпеки суспільства в умовах гібридних загроз (*WARN, 2022*):

> **Компетентність**: здатність адаптувати робочі процеси та особистий простір до складних та непередбачуваних ситуацій, спричинених гібридними загрозами, з урахуванням аспектів соціальної відповідальності.
>
> WARN©

Для того, щоб освітній процес формував таку компетентність, мають бути створені наступні результати навчання:

Перший результат навчання: розуміти комплексну природу, складність, логіку і закономірності гібридних загроз; **Другий результат навчання:** виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії. WARN©

Такі результати навчання неможливо забезпечити лише за рахунок оновлення контенту та інформування про новий тип загроз. Потрібно нарощувати й поведінкові навички – адекватну реакцію на "невідомі невідомі", вміння орієнтуватись у несподіваних ситуаціях, швидко та ефективно надавати відповідь у невизначених складних умовах тощо. Для цього, разом із контентом, мають бути оновлені й практики викладання.

Враховуючи, що гібридні загрози мультидоменні, неочікувані, непрогнозовані, знаходяться нижче порогу ідентифікації та не атрибутований, можна визначити наступні задачі нової методики навчання в умовах гібридних загроз:

1. Підвищення освіченості у різних професійних доменах: оскільки гібридні загрози мультидоменні, то прийняття рішень вимагає системного підходу та розуміння того, як працює вся сукупність доменів; особи, які приймають рішення, мають оцінювати всі окремі загрози та ризики як елементи єдиної "картини", а не аналізувати їх окремо.

2. Розвиток критичного мислення: вміння розрізняти джерела та призначення інформації, обмірковувати, аналізувати та ставити питання, дозволяє уникнути впливу маніпуляцій та окремих агентів, що поширюють неправдиву інформацію.

3. Забезпечення когнітивної стійкості: оскільки гібридні загрози націлені на механізм прийняття рішень, то людська свідомість стає полем бою. Мета когнітивної війни полягає у зміненні

не лише того, що думає людина, а й того, як вона думає і діє (*Хопкінс, 2021*). Когнітивна війна прагне посіяти сумніви, запровадити суперечливі наративи, поляризувати громадську думку, радикалізувати групи і спонукати їх до дій, які можуть зруйнувати або розділити згуртоване суспільство. Нова методика навчання має забезпечити когнітивну стійкість, яка надає людині відчуття та розуміння цінностей та змісту без втрати адаптивності та здібності до розвитку.

4. Нарощування навичок співпраці між різними групами населення, між громадськістю та владою: це передбачає вміння налагоджувати механізми співпраці для спільної роботи над виявленням та протидією гібридним загрозам.

5. Забезпечення інформаційної стійкості, яке формує вміння перевіряти та знаходити достовірну надійну актуальну інформацію.

Вказані навички є у фокусі й звичайних освітніх практик, які розвиваються разом із розвитком людського суспільства. Вони важливі для надання необхідних знань та вмінь, розвитку мислення та налагодження взаємодії та співпраці. Тож, вони мають використовуватись й для навчання в умовах гібридних загроз. Нова методика має на меті спрямувати вибір викладачів у тих педагогічних напрацюваннях, які є особливо корисними для навчання в умовах гібридних загроз, а також на додаток – запропонувати й специфічний методичний підхід до навчання, який містить поєднання змагальних практик в області штучного інтелекту, проактивних педагогічних підходів та спортивного тренування – **інтелектуальний спаринг**.

Гібридні впливи чинять тиск й на сам освітній процес, тому для ефективного навчання в умовах гібридних загроз потрібно врахувати наступні особливості:

1. Використання онлайн-технологій та цифровий твінінг (дублювання): умови гібридних загроз можуть призвести до того, що фізичні зустрічі між викладачами та студентами стають складнішими. Використання онлайн-технологій, таких як відеоконференції та платформи для дистанційного навчання, віртуальні лабораторії тощо, може допомогти зберегти зв›язок між викладачами та студентами та забезпечити продовження процесу навчання.

2. Фокус на здоров›ї та добробуті: умови гібридних загроз можуть призвести до підвищення рівня тривоги та стресу серед студентів та викладачів. Для забезпечення ефективного навчання в таких умовах потрібно подбати не лише про методи донесення чутливого контенту, але й сформувати певну стійкість – підготувати студентів до роботи з таким контентом.

3. Гнучкість та адаптивність: умови гібридних загроз можуть бути дуже непередбачуваними, тому важливо бути гнучким та адаптивним. Це означає, що викладачі та студенти можуть потребувати змінювати свій підхід до навчання та залежно від ситуації швидко реагувати на зміни.

1.2. Окреслюємо межі: термінологія та критерії важливі, як ніколи

Гібридні впливи розмивають системи цінностей, граючи на межі понять. Якщо стерти чітку грань між категоріями (війна-мир, добре-погано, друг-ворог тощо), то виникає "сіра зона" невизначеності, в якій прийняття рішень буде нестійким, потенційно вразливим. Тому викладання дисциплін з тематикою гібридних загроз вимагає уважної роботи з термінологією та критеріями прийняття рішень.

Кейс: визначення поняття «гібридні загрози».

Існує велика кількість визначень "гібридних загроз". Для науки, яка формується, це не є чимось незвичайним. Але у новому безпековому ландшафті навіть розуміння гібридних загроз стає полем бою. Як правило, всі існуючі визначення акцентують увагу на наступних ознаках гібридних загроз:

– мультидоменність, як інструментів, так і вразливостей;

– асиметричність;

– перебування нижче порогу атрибуції, тобто неможливість ідентифікувати діяльність як злочинну і однозначно визначити, хто несе за неї відповідальність.

Це дійсно важливі ознаки. Чи достатньо цього? Скоріш за все, викладач, який обмежиться лише такими ознаками, стикнеться з наступними відповідями:

Студент № 1: "Гібридні загрози відомі з глибокої давнини, в них немає нічого нового, просто технології були іншими: наприклад, отруєння колодязів або підкуп оборонців з тим, щоб вони відкрили ворота фортеці тощо".

Студент № 2: "США проводить гібридну війну проти Ірану та країн Південної Америки".

Студент № 3: "Війна НАТО за Україну – це лише один із етапів гібридної війни, яку Захід розв'язав проти Росії".

Такі відповіді означають, що відбулась підміна поняття: студенти сприйняли асиметричні впливи або комбінацію інструментів як вичерпні ознаки гібридних загроз. Якщо саме такі "знання" студент винесе з освітнього процесу, то він стає **легкою здобиччю маніпуляторів**. Знаючи лише те, що в світі відбуваються асиметричні впливи та приховані операції, такий студент стане ще більш вразливим для теорій змови, перекручення, підміни понять та інформаційно-психологічних операцій гібридних зловмисників.

Неправильне розуміння основних понять гібридних загроз призводить до того, що стійкість студентів буде підірвана навіть більше, ніж якби вони взагалі не проходили навчання.

Рекомендація: при створенні контенту курсів слід спиратись на системні авторитетні дослідження на кшталт тих, що оприлюднює Європейський центр передового досвіду з протидії гібридним загрозам Hybrid CoE, та ретельно опрацьовувати їх зі студентами.

У визначенні Hybrid CoE, "гібридні загрози – це скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів, за використанням широкого кола засобів". Тобто, серед ключових характеристик – націленість таких загроз на вразливості демократії. А чи мають студенти ясне розуміння того, які є особливості та різновиди демократичного способу прийняття рішень? Які демократичні механізми та інституції існують? Що являють собою демократичні цінності? Що є силою демократії та які вона має слабкі місця? Як показала практика, корисним є розгляд конкретних прикладів про те, як реагують на загрози авторитарні та демократичні країни, як-от, наприклад, обговорення COVID-кейсу у контексті проблеми "безпека vs демократичні цінності" (авторитарні та демократичні країни

використовували різні підходи для боротьби з наслідками ковід-пандемії). Часто студенти самі роблять висновки про те, що демократія, надаючи важливі переваги для вільного розвитку суспільства, містить й специфічні вразливості.

Приклади міркувань студентів, які пройшли подібні обговорення та з якими були чітко окреслені особливості демократичних механізмів прийняття рішень:

Студент № 1: "Гібридні загрози – це спроба "хакнути" сучасну демократію, знайти слабину у механізмах прийняття рішень громадою та вдарити саме в її сутність".

Студент № 2: "Не має можливості спрямувати гібридні загрози проти авторитарних країн, бо в них нема таких "органів", які б могли бути вражені цими загрозами".

Студент № 3: "Демократичні країни не можуть відплатити гібридним зловмисникам тією ж монетою, бо, по-перше, у демократіях існують механізми-запобіжники до маніпуляцій, а по-друге, у авторитарних країнах думка громадян не відіграє ролі у прийнятті рішень".

Студент № 4: "Гібридні загрози ставлять демократію перед дилемою безпеки – або потрапити під удари, або згорнути демократію. В таких ситуаціях авторитарним країнам простіше, бо в них лише одне завдання – вийти з-під удару".

Якщо приділити час на обговорення таких суттєвих ознак, це дозволить зняти багато непорозумінь у подальшій роботі. Це дозволить провести чітке розмежування між політичними, інформаційними та військовими операціями (до яких вдається кожна держава) та гібридними впливами (до яких вдаються авторитарні країни-ревізіоністи). А головне – це сформує міцний фундамент для громадської стійкості студентів через обізнаність про справжні загрози.

Висновок: дисципліни з протидії гібридним загрозам вимагають від викладача особливо уважного підходу до термінологічного апарату. Перш ніж переходити до практичних занять та вправ, викладач має впевнитись, що він спілкується зі студентами однією мовою. Для того, щоб зорієнтуватись в термінології, викладачам може стати в нагоді Глосарій, створений в рамках WARN-проєкту (*Гришко та ін., 2021*).

1.3. Підтримуємо етичні системи цінностей

Прийняття рішень базується на певних системах цінностей, які виконують роль внутрішнього арбітра. Система цінностей містить набір параметрів та критеріїв (правил), за якими відбувається прийняття рішень. Проблема виявляється у тому, що системи цінностей розвиваються разом з особистістю, тобто вони не є константами. Можливість оновлення критеріїв вибору відкриває вразливі моменти для маніпуляцій зловмисників.

Це стає серйозною проблемою й для викладача: з одного боку, – заохочувати гнучкість пріоритетів, що створює умови для розвитку особистості; а з іншого – навчити зберігати стійкість системи цінностей та не піддаватись маніпуляціям.

Вирішення цієї проблеми дозволить сформувати головну компетентність, потрібну в умовах гібридних впливів: вміння зберігати не лише сьогоднішню сталу систему цінностей, але й зберігати здатність для її свідомого неманіпулятивного вдосконалення. Все це обумовлює важливість двох моментів, які мають бути враховані у навчальному процесі:

1. Формулювання та обговорення на заняттях етичних принципів та норм в різних сферах професійної діяльності та громадського життя.

2. Розгляд складних прикладів, в яких немає простих рішень, що дозволить підготувати студентів до стійкості в умовах гібридних загроз.

Часто викладачі дисциплін професійного спрямування на своїх заняттях "не встигають" розглянути приклади з етичними викликами, бо крім обмеженого часу аудиторної роботи, ці приклади занадто складні, можуть завести бесіду в неочікуване русло, мають чутливий контент тощо. Це дійсно складні заняття.

До цього додається ще один виклик – такі заняття вимагають нарощування власної стійкості самого викладача. Це – додаткове ретельне опрацювання великої кількості різних аргументів та можливих напрямків розвитку заняття, розуміння етичних принципів прийняття рішень у складних ситуаціях, психологічна рівновага та делікатність.

Але такі складові на заняттях дуже потрібні. Це не обов'язково мають бути окремі модулі чи спеціальні завдання. Акцент на системі цінностей та етично-складних професійних ситуаціях можна додати до будь-якого заняття. Це необхідний елемент для підготовки студентів до роботи в умовах гібридних загроз.

Гібридні загрози часто називають "**злісними проблемами**" (Wicked problem) через те, що такі проблеми складно або неможливо вирішити внаслідок неповноти, суперечності або мінливості інформації і вхідних умов (Cullen, 2018).

Такі проблеми легко стають мішенню гібридних зловмисників, бо злісні проблеми неможливо вирішити. Прийняття рішень у цій площині не буває легким та вимагає міцної системи цінностей, вміння знайти потрібну інформацію та побачити повну картину, розуміння поняття "справедливість" та моральної готовності обирати краще з поганих рішень.

Рішення злісних проблем завжди міститиме негативні наслідки. Але, на відміну від маніпуляцій, стійкість особи, що приймає рішення, має проявлятись у наступному:

– **пильність:** вміння знаходити та обирати джерела інформації з вимогами до достовірності (підтвердження об'єктивності даних), надійності (підтвердження інформації з кількох джерел), авторитетності (підтвердження експертності джерела) та актуальності (своєчасності);

– **свідомий вибір:** вміння формувати та розмірковувати над аргументами;

– **стійкість:** спроможність приймати ефективні обґрунтовані рішення навіть під впливом негативних чинників.

1.4. Вчимо проактивному захисту

Гібридні впливи досягають своєї мети на рівні окремої людини (особи, яка приймає рішення) через когнітивний злам (cognitive hack). Когнітивний злам містить три складові, які можна назвати "3D":

– дезорієнтація: люди втрачають впевненість у своїх цінностях;

– деморалізація: люди стають абсолютно байдужими своїх цінностей ("пофігізм");

– дестабілізація: люди несвідомо руйнують своє середовище на користь зловмисника через неправильні рішення.

Для того, щоб наш розум створив імунітет проти когнітивного зламу, який є основою гібридних впливів, потрібна "академічна вакцина". Так само, як імунітет людини, захист від гібридних загроз вимагає не лише вміння протидіяти вже відомим загрозам (так званим "відомим невідомим"), але й виявляти та протидіяти "невідомим невідомим" – тобто таким новим типам випливів, навіть про існування яких ніхто не обізнаний.

Інформація про "Невідомі невідомі" не піддається моніторингу, який побудованій на сприйнятті того, що ми очікуємо сприймати (за допомогою шаблонів розпізнавання або використання набору індикаторів). Це пов’язано з тим, що аналітик ніколи раніше не бачив цієї закономірності і не може мати набір індикаторів для того виду атаки, який раніше ніколи не мав місця або навіть не був уявним. Проблема захисту системи в умовах "невідомих невідомих" атак добре знайома спеціалістам в області кіберзахисту: сукупність технологій, яка використовується в антивірусному програмному забезпеченні для превентивного виявлення потенційно небезпечних вразливостей, створює механізм **проактивного захисту**. Такий принцип стане в нагоді й для захисту осіб, які приймають рішення в умовах гібридних загроз (**рис. 1**).

Проактивна безпека запобігає невідомим раніше атакам. Вона допомагає усувати будь-яку вразливість, яка робить нас сприйнятливими до атак, перш ніж злочинці використають їх.

Рис. 1 дозволяє виявити ключові підходи, які мають бути втілені у навчанні для забезпечення навичок проактивного захисту:

– моделювання поведінки супротивника: потрібно навчити студентів виходити за межи власної позиції і "залазити у шкуру" ворога;

– симуляція атак, протидії, суперництва, спарингів та інших видів конкурентної інтерактивності.

Це означає, що пасивного слухання матеріалу недостатньо для протидії гібридним загрозам. Це вимагає **активного навчання** (Active learning), тобто залученості студентів до емпіричних

завдань. Існує багато форм активного навчання, серед яких корисними для навчання проактивному захисту, є наступні:

1. Експериментальне навчання (experiential learning, ExL) – філософія та методологія, згідно з якою викладачі цілеспрямовано взаємодіють зі студентами у практичному досвіді та зосередженій рефлексії, щоб збільшити знання, розвинути навички та роз'яснити цінності (*Northern Illinois University, 2012a*). Існує велика кількість підходів та методів експериментального навчання, серед яких в умовах гібридних загроз особливу увагу привертають:

– **симуляція** (simulation), яка дозволяє розвивати критичне мислення, самостійне навчання та є ефективним засобом боротьби з неправильними уявленнями студентів (*Caniglia, 2019*). Метод передбачає створення ситуацій, які вимагають швидкої реакції та дії, які стимулюють студентів до проактивної поведінки;

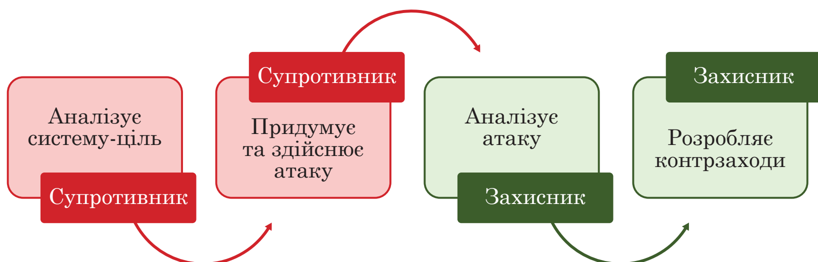
– **рольові ігри** (role-playing): техніка, яка дозволяє студентам досліджувати реалістичні ситуації, керовано взаємодіючи з іншими людьми, щоб отримати досвід і випробувати різні стратегії у певному середовищі (*Glover, 2014*). Цей підхід дозволить студентам побувати зловмисником, але не стати зловмисником. Не можна зрозуміти, як діятиме ворог, якщо не змоделювати його поведінку, не програти можливі сценарії омани, маніпуляції, перекручування, не спробувати атакувати. У такому навчанні важливо зберігати власну систему цінностей. Саме входження у роль та вихід з неї дозволять зрозуміти ворога, але залишитись собою.

2. Діяльне навчання (action learning) – навчання через вирішення конкретної проблеми, який включає виконання дій і рефлексію над результатами (*Corporate Finance Institute, 2022*).

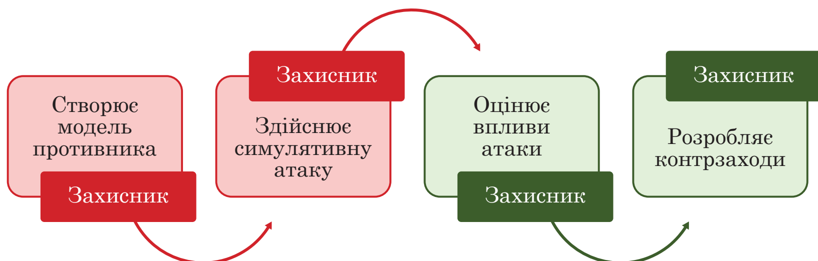
3. Групове або кооперативне навчання (cooperative learning) – метод навчання, що оснований на співробітництві студентів у групах. При такому підході студенти досягають успіхів у навчанні, лише за умови ефективної взаємодії між собою (*SERC Pedagogic Service, n.d.*)

4. Навчання служінню (service-learning) – освітній підхід, який поєднує цілі навчання з громадською роботою (волонтерством), щоб забезпечити прагматичний, прогресивний досвід навчання, одночасно задовольняючи потреби суспільства (*Suffolk University, n.d.*).

5. Ситуаційне навчання (situated learning) – студенти навчаються, беручи активну участь у вирішенні проблем, які формуються у реальних життєвих ситуаціях (*Northern Illinois University, 2012b*).



а) створення реактивного захисту



б) створення проактивного захисту

Рис. 1. Підходи до створення реактивного та проактивного захисту
Складено за Biggio et al., 2014

Ці підходи безсумнівно мають користь для формування у студентів компетентності з протидії гібридним загрозам. Особливості їх застосування та деякі приклади будуть запропоновані до розгляду у наступних розділах.

Джерела посилань

Action Learning (2022). Corporate Finance Institute. Available at: https://corporatefinanceinstitute.com/resources/elearning/action-learning/

Biggio, B., Fumera, G., Roli, F. (2014). Pattern recognition systems under attack: design issues and research challenges. International Journal of Pattern Recognition and Artificial Intelligence, 28 (7), 1460002. doi: https://doi.org/10.1142/s0218001414600027

Caniglia, J. (2019). Simulations as a Teaching Strategy. Kent State University Center for Teaching and Learning. Available at: https://www.kent.edu/ctl/simulation-teaching-strategy

Concept of Comprehensive Security – Building National Resilience in Finland. Turvallisuuskomitea. Available at: https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/

Cooperative learning. Pedagogy in Action, National Science Digital Library. SERC Pedagogic Service. Available at: https://serc.carleton.edu/sp/library/cooperative/index.html

Countering hybrid threats (2023). NATO. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

Cullen, P. (2018). Hybrid CoE Strategic Analysis 8: Hybrid threats as a new 'wicked problem' for early warning. Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

Digital Education Action Plan 2021–2027: Resetting education and training for the digital age (2020). European Council, European Commission, European Economic and Social Committee. Available at: https://education.ec.europa.eu/focus-topics/digital-education/action-plan

Experiential Learning (2012). CITL, Center for Innovative Teaching and Learning. Northern Illinois University. Available at: https://www.niu.edu/citl/resources/guides/instructional-guide/experiential-learning.shtml

Glover, I. (2014). Role-play: An Approach to Teaching and Learning. Technology Enhanced Learning at Sheffield Hallam University.

Available at: https://blogs.shu.ac.uk/shutel/2014/07/04/role-play-an-approach-to-teaching-and-learning/

Gobert, C. (2022). What Is Service-Learning? The Center for Community Engagement, Suffolk University. Available at: https://www.suffolk.edu/student-life/student-involvement/community-public-service/service-learning/what-is-service-learning

Hagelstam, A. (2018). Cooperating to counter hybrid threats. NATO Review. Available at: https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Joint Framework on Countering Hybrid Threats (2016). European Council, European Commission, NATO. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

Situated learning (2012). CITL, Center for Innovative Teaching and Learning. Northern Illinois University. Available at: https://www.niu.edu/citl/resources/guides/instructional-guide/situated-learning.shtml

Updated study programmes. WARN. Available at: https://warn-erasmus.eu/ua/deliverables/updated-study-programmes/

Гришко, С. В., Головянко, М. В., Титаренко, М., Чех, М., Василиця, О., Ланюк, Є. та ін.; Гришко, С. В. (Ред.) (2021). Глосарій з гібридних загроз. Erasmus+ Capacity Building Project WARN, 113.

Хопкінс, Дж. (2021). Протидія когнітивній війні: інформованість і стійкість. НАТО рев'ю. Available at: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html

ЛЕКЦІЙНЕ ЗАНЯТТЯ

Оксана Карпенко[1]

[1]Державний університет інфраструктури та технологій

Як показала практика, викладання курсів з протидії гібридним загрозам стикається з потужним методичним викликом щодо подачі теоретичного матеріалу:

– з одного боку, проактивний захист (який є головним фокусом такого навчання) вимагає якомога більше практичної підготовки. Зазвичай, така вимога задовольняється через перерозподіл аудиторного навантаження (за рахунок зменшення лекційних занять). Це змушує шукати нестандартні форми подачі теорії, зокрема – й поза аудиторією;

– з іншого боку, студент не зможе навчитись захисту в умовах гібридних загроз лише через практичні вправи, без системного розуміння того, що відбувається у широкому середовищі (а не в локальному осередку). Тобто "бачення без дії – це мрія, а дія без бачення – це жахіття" (східна народна мудрість). Захист від гібридних загроз у першу чергу вимагає комплексної обізнаності осіб, які приймають рішення. Без попереднього опанування теоретичного матеріалу неможливо досягти такого ефекту. Саме тому не можна відкидати жодного педагогічного напрацювання, бо кожний спосіб подачі теоретичного матеріалу може стати у нагоді при викладанні курсів з протидії гібридним загрозам.

Таким чином, серед педагогічних напрацювань потрібно обрати такі рішення, які: (1) дозволяють відповісти на виклик, пов'язаний з подачею теоретичного матеріалу, тобто як помістити великий обсяг мультидисциплінарної теорії у невеликий обсяг часу; (2) надають викладачеві можливість вибору залежно від аудиторії та особливостей курсів; (3) створюють умови для комбінації

існуючих підходів або для адаптивного формування нових підходів до подачі матеріалу.

Технології завжди відігравали важливу роль у навчанні, але вони, як правило, використовувалася лише для підтримки звичайного навчання. Сучасні тенденції надають можливість змінити сам підхід до організації лекційних занять. Це важливо в умовах гібридних загроз, коли навіть знайомство з теоретичним матеріалом вимагає інтерактивного спілкування та проактивності студентів.

Можна виділити такі підходи до організації лекційних занять з використанням новітніх інформаційних технологій (*Bates, 2015; с. 614*):

– **змішане навчання** (blended learning), коли технічні засоби підтримують навчальний процес та не вимагають його перепланування (проведення слайд-лекцій, використання системи управління навчанням для підтримки викладання в аудиторії, для зберігання навчальних матеріалів, тестів та онлайн-обговорень);

– **гібридне або гнучке навчання** (hybrid or flexible learning) – потребує перепланування викладання, щоб студенти могли виконувати більшу частину свого навчання в Інтернеті, приходячи в аудиторію лише для дуже специфічного особистого навчання, наприклад лабораторних або практичних робіт, які неможливо виконати задовільно онлайн;

– **онлайн навчання** (fully online learning) – тобто навчальний процес без навчання в аудиторії, зокрема – курси з отриманням кредитів (дистанційна версія аудиторної освіти); некредитні курси, які пропонуються лише в Інтернеті, наприклад, курси безперервної професійної освіти; повністю відкриті курси, такі як MOOC; та відкриті освітні ресурси, доступні для безкоштовного завантаження в Інтернеті, до яких викладачі або студенти мають доступ для підтримки викладання та навчання.

Гібридне навчання та онлайн навчання передбачають повну перебудову дизайну курсів. При такій організації час на лекційні заняття має бути максимально зменшений (*Bates, 2015; с. 615*). Для того, щоб ефективно донести до аудиторії теоретичний матеріал та використати його у подальшій практичній роботі для протидії гібридним загрозам, слід звернути увагу на наступні підходи:

– "**перегорнуте навчання**" (англ. flipped classroom) – технологія навчання, коли основне засвоєння нового матеріалу відбувається самостійно, а час аудиторної роботи виділяється на виконання завдань, вправ, проведення лабораторних і практичних досліджень, індивідуальних консультацій. Таким чином, традиційне представлення лекції перевтілюється в її обговорення, у якому розкриваються дискусійні питання, презентуються проекти, виконуються практичні роботи тощо, а відео-лекція при такому підході стає ключовим компонентом (*Приходькіна, 2014*);

– **відкриті освітні ресурси** (Open educational resources, OER) – одна з розробок відкритої освіти (open education) у вигляді цифрових навчальних матеріалів, які знаходяться у вільному доступні в Інтернеті; викладачі та студенти можуть безкоштовно завантажувати та, за необхідності, адаптувати чи змінювати відповідно до ліцензії Creative Commons, яка забезпечує захист для творців матеріалу;

– **масові відкриті онлайн-курси** (MOOC) – інтернет-курси з масштабною інтерактивною участю та відкритим доступом через інтернет. На додаток до традиційних матеріалів навчального курсу, такі як відео, читання, і домашні завдання, MOOC надає можливість використання інтерактивної взаємодії користувачів, які допомагають створити спільноту студентів, викладачів та асистентів. Для MOOC характерна відкрита та проста реєстрація, великі обсяги аудиторії (від 1000 до 100 000), вільний доступ до відеозаписів лекцій, комп'ютерне оцінювання з моментальним зворотнім зв'язком.

Існують два принципово різні типи MOOCs (*Fidalgo-Blanco et al., 2016*):

1. **xMOOC** – це класичний курс на основі платформ е-навчання, в якому є початок і кінець, є лекції, інтерактивні тести та розділ для інтерактивного обговорення. Тут студенти мають дотримуватися термінів виконання завдань. Тобто xMOOC орієнтуються на більш традиційний, академічний підхід до освоєння матеріалу.

2. **cMOOC** ("c" – connectivism) – курси по принципу соціальних мереж, які засновані на спілкуванні учасників та обговоренні певних тем. Підхід базується на теорії з'єднувальних знань (connective knowledge). Це передбачає мережеву взаємодію та використання технологій Web 2.0 для пошуку знань, навчальних спільнот та

людей зі подібними інтересами, щоб створювати та розвивати різні сфери знань. Тут викладач стає модератором, який заохочує подібні контакти та самостійно збирає та аналізує, акумулює, розшарює зібраний матеріал. Такий підхід має більшу гнучкість і чутливість, а також забезпечує соціалізацію учасників – пошук однодумців та можливість розширення мережі контактів.

Одним з ефективних способів організації гібридного та онлайн навчання є створення відео-лекцій. Це дозволяє зробити лекційний матеріал доступним для повторного перегляду у будь-який час. Створення відео-лекцій може відбуватись:

– проведенням автоматичного запису лекцій, які проходять в аудиторії, щоб студенти могли повертатись до проведених занять;

– попередній запис лекції для того, щоб студенти дивилися їх самостійно з наступним обговоренням в аудиторії.

Для підготовки відеоматеріалу лекцій про гібридні загрози слід звернути увагу на практику створення **TED-лекцій (TED Talk)**. Організатори збирають TED-конференції, щоб просувати ідеї, які мають змінити світ. Специфіка формату TED-лекцій привернула увагу всього світу та зробила їх окремим явищем просвітництва:

– в якості спікерів запрошують найяскравіших особистостей (вчених, філософів, музикантів, меценатів, бізнесменів тощо);

– спіч-лекція триває не більш ніж 18 хвилин, протягом яких доповідачі мають донести своє послання аудиторії, що зібралася; лекція має бути не просто цікавою – вона має надихати та захоплювати;

– ці натхненні виступи можна дивитись не лише наживо: їх транслюють онлайн, записують та викладають у мережу для безкоштовного використання на платформі TED.com;

– обов'язковим є супровід слайдами / субтитрами із базовими визначеннями, класифікаціями і т.п., що надає можливість одночасно і слухати, і читати;

– до кожного відео надається не лише список літератури, а ще й перелік посилань на фільми, події, історії, які ілюструють матеріал.

Важливо зазначити, що який би підхід не обирав лектор, діяльність викладача на всіх етапах підготовки й проведення лекцій має орієнтуватися на логіку сучасних дидактичних технологій. Формат лекцій залежить від:

– прогностичності цілей навчання (чому навчати і для чого навчати?);

– з урахуванням рівня кваліфікації викладача (хто навчає?);

– особливостей аудиторії (кого навчає?);

– відбору і проектування змісту освіти (який саме матеріал давати?);

– форм організації навчального процесу (як навчати?);

– методів і засобів навчання (за допомогою чого?);

– діагностики досягнутих результатів (що вийшло?).

Саме такі підходи дозволяють найбільш виважено і раціонально використовувати таку форму навчання, як лекції, що за своїм рівнем відповідають вимогам підготовки висококваліфікованих фахівців.

Джерела посилань

Bates, A. W. (2015). Teaching in a digital age: Guidelines for designing teaching and learning. BCcampus.

Fidalgo-Blanco, Á., Sein-Echaluce, M. L., García-Peñalvo, F. J. (2016). From massive access to cooperation: lessons learned and proven results of a hybrid xMOOC/cMOOC pedagogical approach to MOOCs. International Journal of Educational Technology in Higher Education, 13 (1). doi: https://doi.org/10.1186/s41239-016-0024-z

Приходькіна, Н. О. (2014). Використання технології "перевернутого" навчання у професійній діяльності викладачів вищої школи. Науковий вісник Ужгородського національного університету. Серія: Педагогіка. Соціальна робота, 30, 141–144. Available at: http://nbuv.gov.ua/UJRN/Nvuuped_2014_30_53

3. ПРАКТИЧНЕ ЗАНЯТТЯ

Світлана Гришко[1]
Ольга Копієвська[2]
[1]Харківський національний університет радіоелектроніки
[2]Національна академія керівних кадрів культури та мистецтв

Перенесення центру ваги на практичні заняття у навчанні є загальною тенденцією сучасності (*Bates, 2015; p. 168*). Але навчання в умовах гібридних загроз робить принципово важливим не пасивне споживання інформації, а саме активне залучення студентів до опрацювання матеріалу та застосування його в різних практичних ситуаціях.

Специфіка гібридних загроз вимагає надання студентам навичок:

– прийняття рішень як в зрозумілих ситуаціях, так і в аномальних;

– роботи індивідуально та в групі, формування навичок соціальних комунікацій для вирішення проблем;

– роботи в умовах запасу часу та дефіциту часу.

Такі навички формуються під час практикування активних дій. Тому різні форми практичних занять є невід›ємним елементом навчання в умовах гібридних загроз.

Протидія гібридним загрозам, які націлені на механізми прийняття рішень, вимагає когнітивного захисту. Це означає, що студенти мають навчитись самостійно добувати або конструювати знання на основі академічних критеріїв, таких як логіка, докази та аргументи. Розвиток критичного мислення вчить студентів думати про світ по-іншому. Для досягнення таких завдань важливе значення мають **розмова та обговорення**. Важливо, щоб студенти навчались через взаємодію та обговорення між собою, щоб отримати навички побудови соціальних контактів через поєднання власних

індивідуальних інтересів з інтересами інших учасників. Навчання, яке відбувається через діалог, має стати невід›ємним елементом на курсах з протидії гібридним загрозам.

Діалогічне навчання (dialogical learning) – це навчання через діалог, в якому різні люди надають аргументи, засновані на претензіях на обґрунтованість, а не на владу (*Kincheloe & Horn, 2007, p. 552*). Різноманіття форм діалогічного навчання дозволяє підібрати ті аргументи, які відповідають специфіці та завданням конкретного навчального процесу, наприклад:

– **семінарські заняття:** це форма навчання, під час якої студенти обговорюють матеріал, який був викладений на лекції, у групі під керівництвом викладача;

– **дискусії:** під час дискусій студенти висловлюють свої думки щодо певної проблеми або теми, інколи під час цього процесу можуть змінювати своє ставлення до певної теми;

– **суперечливі дискусії:** це форма діалогічного навчання, під час якої студентам пропонується висловити свої аргументи "за" та "проти" певної тези, що дозволяє розвивати навички аргументації та доказовості;

– **круглий стіл:** це форма діалогічного навчання, під час якої студенти засідають за круглим столом і обговорюють певну тему, обмінюються думками.

Іншою невід'ємною складовою курсів з протидії гібридним загрозам має стати забезпечення практичної активності студентів, яка забезпечується різними підходами:

– "**навчання через дію**" (Learning by doing) базується на тому, що найбільш ефективним способом навчання є активна участь студентів у практичних завданнях, дослідженнях та інших формах практичного досвіду. Навчання відбувається як осмислення власного досвіду, особливо того досвіду, де студенти беруть активну участь у створенні речей і дослідженні світу (*Bruce & Bloch, 2012*);

– "**навчання на основі проблем**", проблемно-орієнтований підхід (Problem-based learning) – передбачає вирішення студентами реальних проблем, які виникають у певній області знань, та допомагає розвивати їхні навички самостійного пошуку інформації та аналізу, а також попрактикуватись у розв’язанні реально

існуючих проблем. До того ж вирішення реальних проблем дає відчуття відповідальності. Але й слід врахувати, що для студентів цей підхід може виявитись складним, якщо їх база знань недостатня, та призвести до "когнітивного перевантаження" (cognitive overload);

– "**навчання на основі кейсів**" (Case-based learning) – використовує реальні або вигадані сценарії, щоб допомогти студентам зрозуміти теорію та її практичні застосування. Студентам пропонується аналізувати та розв›язувати проблеми, що виникають у цих сценаріях.

Існує велика кількість підходів до **навчання через дію** (Learning by doing), серед яких можна визначити наступні:

– **лабораторні роботи, робота в майстерні або студії:** студенти отримують можливість виконувати практичні завдання та дослідження у контрольованому середовищі, що надає їм можливість побачити теорію "в дії", перевірити гіпотези та впевнитись, наскільки добре працюють концепції, теорії чи процедури. Це можуть бути різні формати, наприклад:

1) "**мокрі лабораторії**" (Wet labs) – лабораторні заняття, де студенти працюють з реальними зразками та речовинами (звідси й назва), використовуються, зазвичай, при навчанні природничих наук, зокрема біології, хімії та фізики, для проведення експериментів (аналіз проб рідин, культивування мікроорганізмів, синтезу речовин, тестування нових матеріалів тощо). Wet labs вимагають спеціального обладнання та матеріалів, а також від студентів дотримання правил безпеки;

2) **віддалені лабораторії** (Remote labs) – дозволяють студентам проводити експерименти та дослідження за допомогою віддаленого доступу до реального обладнання, яке знаходяться в іншому місці, або симуляцій. Це вимагає використання веб-камер, мережевого з’єднання, відеоконференцій, програмного забезпечення для збору даних, спеціального фізичного обладнання тощо.

З точки зору протидії гібридним загрозам, важливо, що лабораторія (студія, майстерня) знайомить студентів із критично важливим культурним аспектом науково-технічного дослідження: всі ідеї мають бути перевірені суворим і особливим чином, щоб їх верифікувати (вважати істинними);

– **практика** у реальному середовищі: студенти отримують можливість **спостерігати** за процесами та вчитися розв'язувати проблеми, що виникають в реальному житті;

– **стажування:** студенти отримують можливість **працювати** у реальному середовищі, знайомитися з певною галуззю, брати участь у робочому процесі та у вирішенні проблем, що виникають у роботі;

– **змагання та конкурси:** студенти можуть брати участь у суперницькій взаємодії, де вони можуть використовувати свої знання та навички для конкурентного вирішення завдань та проблем;

– **рольові ігри та симуляції:** студенти грають ролі та вирішують завдання, які схожі на ті, що можуть зустрітися у реальному житті, що дозволяє їм навчитися приймати рішення та розв›язувати проблеми у непередбачуваних ситуаціях.

В умовах гібридних загроз набувають актуальності такі **форми роботи студентів**:

– **групові** проекти та завдання, спільне навчання (cooperative learning) передбачають, що студенти об'єднуються, обговорюють ситуацію та вирішують проблеми спільно (*Dishon & O'leary, 1984*). Це допомагає розвивати навички взаємодії, співпраці та комунікації. Це може також сприяти розвитку навичок стійкості та пильності, оскільки студенти мають виконувати завдання у межах визначеного часу та зосереджуватись на досягненні спільного результату;

– вправи на **розвиток уваги та концентрації**, які можуть бути організовані окремо або включені до різних типів занять;

– **гейміфікація** – включення елементів ігрового дизайну в освітнє середовище (*Dichev & Dicheva, 2017*). Елементами гейміфікації є таблиці лідерів, нагородні бали, значки, наклейки тощо. Гейміфікація збільшує участь, залучення та конкуренцію. Гейміфікація стимулює учнів до навчання та практикування, створює інтерактивне середовище в аудиторії та спонукає студентів щоразу працювати краще.

Більш складною формою практичного навчання студентів є **«Навчання на основі проектів», проєктно-орієнтована (Project-based learning)** форма навчання, де студенти отримують можливість вести наукові дослідження та виконувати проєкти, які вимагають від них застосування *комплексу різних знань та навичок*,

щоб дійти до певного результату (*Project Based Learning, n.d.*). Така міждисциплінарність є корисною практикою в умовах гібридних загроз, які також характеризуються мультидоменністю та мультиінструментальністю.

Крім того, "Навчання на основі проєктів" сприяє розвитку сукупності аналітичних, дослідницьких та презентаційних навичок. Під час роботи над проєктом, студенти працюють у команді та вирішують реальні проблеми, що вимагають пошуку інформації, аналізу, дослідження та створення конкретного продукту або рішення. А створення проєктів, які потребують довготермінового планування та виконання, допоможе студентам розвивати навички пильності, витривалості та терпіння.

Допоміжнім методом навчання студентів у складних непередбачуваних умовах гібридних загроз може стати наставництво.

Наставництво (mentorship, apprenticeship) – це процес, у якому більш досвідчений наставник допомагає менш досвідченому учню у розвитку його знань та навичок. Цей підхід може використовуватися у комбінації з іншими методами навчання та забезпечує індивідуальний підхід до кожного студента.

Викладачеві під час **організації практичних завдань та занять** в умовах гібридних загроз важливо звернути увагу на низку особливостей:

1. Орієнтація на потреби студентів: знаходження у сфері того, чим живуть студенти, забезпечить максимальну увагу та зацікавленість під час практичних вправ та користь від навчання.

2. Активна участь студентів: залучення до вирішення практичних завдань, взаємодії з іншими студентами, обговорення проблем та пошук їх рішень стає обов›язковою умовою навчання в умовах гібридних загроз, тому викладачеві потрібно забезпечити таку залученість через присутність, доступ студентів до технологій, ресурсів (мається на увазі як онлайн-технології навчання, так і технології, які вивчаються під час занять).

3. Фокус на практичному застосуванні знань: теоретичний матеріал має допомагати студентам застосовувати отримані знання на практиці, надавати можливість практикувати нові навички та отримувати фідбек від викладачів.

4. Використання сучасних технологій: інтерактивні технології, онлайн-інструменти, симуляції допомагають підвищити ефективність практичних занять та зробити їх більш захоплюючими та динамічними.

5. Оцінка результатів: всі практичні заняття, вправи та завдання повинні мати ясні цілі та визначені критерії оцінювання, які дозволять визначати об›єктивні результати, відстежувати прогрес студентів та забезпечувати регулярний контроль їх роботи. Це – важливий стимул для досягнення цілей навчання та розвитку навичок стійкості та пильності.

Джерела посилань

Bates, A. W. (2015). Teaching in a digital age: Guidelines for designing teaching and learning. BCcampus.

Bruce, B., Bloch, N.; Seel, N. M. (Ed.) (2012). Learning by Doing. Encyclopedia of the Sciences of Learning. Boston: Springer, 1821–1824. doi: https://doi.org/10.1007/978-1-4419-1428-6_544

Dichev, C., Dicheva, D. (2017). Gamifying education: what is known, what is believed and what remains uncertain: a critical review. International Journal of Educational Technology in Higher Education, 14 (1). doi: https://doi.org/10.1186/s41239-017-0042-5

Dishon, D., O'leary, P. W. (1984). A Guidebook for Cooperative Learning: A Technique for Creating More Effective Schools. Holmes Beach: Publication Sales, Learning Publications, Inc.

Kincheloe, J. L., Horn, R. A. (Eds.) (2007). The Praeger handbook of education and psychology. Vol. 4. Greenwood Publishing Group.

Project Based Learning. Available at: https://www.pblworks.org/what-is-pbl

4. ВОРКШОП ТА МАЙСТЕР КЛАС

Тетяна Борозенцева[1]
[1]Горлівський інститут іноземних мов

Майстер-клас та воркшоп є двома різними форматами навчальних заходів, які часто використовуються для передачі знань та навичок у практичний спосіб.

Воркшоп зорганізується та проводиться як практичне дослідження, що зосереджене на окремій та неоднозначній проблемі і здійснюється групою людей, зусилля яких певним чином організовані; це дозволяє розглянути проблему цілісно, під різними, нестандартними кутами зору (**табл. 1**).

Завдання воркшопу:

– допомогти актуалізувати досвід, наявний в учасників групи;

– спираючись на наявні ресурси, інтегрувати нову позицію розуміння та аналізу проблеми, що розглядається групою;

– покращити здатність учасників розв'язувати подібні проблеми.

Принципи роботи у форматі воркшопу:

– залучення учасників до активної співпраці та самостійного пошуку рішення проблеми;

– миттєвий зворотній зв›язок (бути завжди поряд с учасниками);

– заохочення розбіжності у думках, мотивація студентів вчитися один у одного;

– підтримка шанобливої форми висловлювання критичних суджень.

Майстер-клас передбачає попередню демонстрацію ведучим практичних прийомів та методів вирішення проблем за означеною тематикою, організацію процесу відпрацювання запропонованих практичних технологій в індивідуальному чи груповому форматі та

обговорення результатів роботи (*Єрмола & Василенко, 2006*). У якості ведучих долучаються партнери-експерти, які мають практичний досвід вирішення питань, пов'язаних із запобіганням гібридних загроз в окремій сфері.

Таблиця 1. Структура воркшопу

Назва етапу	Завдання	Результат етапу
Вступна частина	Знайомство учасників, обговорення правил роботи, регламенту. Оголошення теми, мети, очікувань та критеріїв результату заняття	Створення невимушеної атмосфери для навчання (відкритість для запитань та пропозицій)
Інформаційна частина	Надання актуальної та практичної інформації стосовно запланованої теми обговорення. Постановка проблеми	Введення учасників у розуміння проблеми. Створення зацікавленості у її розв'язанні
Практична частина	Організація процесу самостійного пошуку рішення проблеми (робота в малих групах, загальна дискусія, брейншторм тощо)	Знаходження оригінальних ідей, корекція та консолідація точки зору учасників
Підбиття підсумків	Узагальнення змістовних результатів роботи. Зворотній зв'язок від учасників	Емоційне підкріплення набутого досвіду з теми навчання

Головне завдання майстер-класу – узагальнити та поширити розроблену авторську технологію за проблематикою протидії гі-

бридним загрозам. В процесі навчання йде безпосереднє обговорення запропонованого методичного продукту та апробація його використання учасниками заняття.

Приклад тематики майстер-класу (*Данилюк, 2021; Freedman et al., 2021; Mazaraki et al., 2021*):

– техніки аналізу засобів та заходів ідеологічної дезорієнтації та розкладання свідомості певних груп людей з метою зниження їх ідейної, політичної, духовної та морально-психічної стійкості;

– прийоми запобігання інструментам впливу ворожих спецслужб (компрометація, дезінформація, науково-технічна розвідка та розвідка у ЗМІ противника, агентурне проникнення, вербування);

– технології викриття дезінформації, яка використовується для дестабілізації суспільства шляхом прямих атак на цивільні території та спроб спровокувати поляризацію та заворушення;

– методика виявлення підривної діяльності на основі розвитку мережі спеціалістів центральних органів державної влади у кожній сфері державного управління та суспільного життя та ін.

Методика проведення майстер-класів здебільшого не має єдиних норм і залежить від рівня інтуїції провідного фахівця і ступеню сприйнятливості слухачів. При цьому хід майстер-класу повинен спиратись на певну структуру, яка гарантує якісне виконання завдань заходу, а саме: відтворення ведучим власної технології в тематиці протидії гібридним загрозам; навчання учасників майстер-класу конкретним навичкам, що становлять основу транслъованого аналітичного досвіду; популяризація інноваційних ідей, авторських знахідок в означені сфері; надання допомоги учасникам майстер-класу у визначенні завдань їх власного подальшого самовдосконалення в напрямі опанування технології запобігання гібридним загрозам.

Активізація пізнавальної діяльності учасників майстер-класу, ефективне практичне освоєння найважливіших навичок у рамках демонстрованого досвіду забезпечується:

– виразністю інноваційної ідеї майстер-класу та культурою її презентації ведучим;

– вибором, повнотою, прогресивністю та оригінальністю запропонованої технології;

– здатністю мотивувати до включення кожного учасника в активну творчу роботу зі створення нового продукту діяльності на занятті;

– технологічністю запропонованих процедур аналізу інформації та синтезу нових ідей, етапів самоаналізу та самокорекції дій учасниками майстер-класу;

– загальною ерудицією та культурою спілкування ведучого, нестандартністю мислення, здатністю до імпровізації.

Воркшоп і майстер-клас базуються на одному тому самому принципі – "навчання через практику". Але, як бачимо, вони по різному реалізують цей принцип у навчальному процесі.

Майстер-клас проводиться одним або кількома експертами, фокусується на демонстрації та показі певних технік, методів або процесів у практичній формі, де учасники досить пасивно спостерігають, сприймають запропоновану інформацію та демонстрацію від експерта, і потім залучаються до практичного відтворення презентованого досвіду, готової технології.

Воркшоп також проводиться експертами, але він передбачає активну роботу учасників, має інтерактивний характер, спрямований на взаємодію та вирішення конкретних завдань або проблем. На відміну від майстер-класу, учасники воркшопу активно залучаються до творчої діяльності, яка передбачає креативний пошук шляху виконання практичних завдань.

Ще однією відмінністю можна вважати регламент занять: майстер-клас завжди має чіткий початок та завершення демонстрації тієї чи іншої технології, а воркшоп може надавати студентам можливість долучатись до виконання практичних вправ у будь-який зручний момент (за аналогією з майстернею, де людина має змогу творити будь-коли).

Таким чином, майстер-клас має на меті познайомити учасників з конкретними технікам або прийомами, а мета воркшопу – сприяти практичному навчанню та формуванню практичних навичок, обміну досвідом, створенню нових ідей та спільному вирішенню проблем.

Воркшоп та майстер-клас можуть поєднуватись під час організації занять, створюючи велику кількість різноманітних гібридних форм для навчання через практику.

Джерела посилань

Freedman, J., Hoogensen Gjørv, G., Tahinjanahary Razakamaharavo, V. (2021). Identity, stability, Hybrid Threats and Disinformation. Revista ICONO14 Revista Científica de Comunicación y Tecnologías Emergentes, 19 (1), 38–69. doi: https://doi.org/10.7195/ri14.v19i1.1618

Mazaraki, A., Kalyuzhna, N., Sarkisian, L. (2021). Multiplicative effects of hybrid threats. Baltic Journal of Economic Studies, 7 (4), 136–144. doi: https://doi.org/10.30525/2256-0742/2021-7-4-136-144

Данилюк, О. В. (2021). Методика раннього виявлення гібридних загроз в умовах агентурних заходів впливу РФ. Актуальні Проблеми Політики, 67, 135–142. doi: https://doi.org/10.32837/app.v0i67.1164

Єрмола, А. М., Василенко, О. М. (2006). Технологія організації науково-методичної роботи з педагогічними кадрами. Харків: Курсор, 312.

5. БРЕЙНШТОРМ ТА СИМУЛЯЦІЯ

Павло Худ[1]
[1]Український католицький університет

Брейншторм

Брейншторм є одним із методів сприяння груповій креативності, за допомогою якого учасники спонтанно обмінюються ідеями та думками з метою прийняття рішень (*Al-Samarraie & Hurmuzan, 2018; Gogus, 2012*).

Особливістю методики брейншторму є те, що вона дозволяє усім або максимальній кількості учасників висловити своє бачення стосовно якоїсь вже існуючої ідеї чи теми.

Брейншторм важливий, коли у вас є уявлення про бажаний результат, але не видно чіткого рішення. Саме у такій ситуації є сенс використовувати брейншторм як навчальну методику, щоб разом із студентами подумати над різноманітними, навіть божевільними ідеями, поки ви не знайдете те, що працює (*Roth, 2015*).

Помилкою є використання брейншторму на етапі генерування нових ідей, через що ця методика може виглядати хаотичною і часто від неї відмовляються. Через це, техніка мозкового штурму перетвориться на простір перекрикування один одного, суперечки щодо того, чия думка правильна, а чия неправильна. У підсумку зростає ризик того, що буде ухвалено абсурдне рішення, або запропоновано абсурдну ідею (*Кнапп et al., 2016*).

Брейншторм є інструментом, який можливо добре використовувати у процесі прийняття рішення. Він складається з трьох компонентів: генерування ідей для нових рішень, тестування ідей нових рішень та впровадження нових ідей, щоб знайти найбільш оптимальне рішення.

Методика брейншторму застосовується на етапі тестування ідеї. Окрім брейншторму, у процесі тестування ідей також можна використовувати методику прототипування. На етапі тестування ідеї важливо бути скептичним до висловленої напередодні ідеї. Брейншторм має допомогти з'ясувати, що потрібно змінити в ідеї, щоб вони стала ще кращою та ефективнішою.

При формуванні команд для брейншторму важливо звернути увагу на те, щоб до її складу увійшли учасники з різним досвідом та знаннями. Завдяки цьому учасники брейншторму зможуть надбудовувати нові ідеї на основі існуючих, а не сперечатися між собою, чия ідея краща.

Важливо, щоб під час занять викладачі створили атмосферу, коли думки студентів довкола запропонованих раніше ідей допомагали створювати нові рішення, хоч якими б дивовижними вони не здавалися у момент обговорення.

Ніхто з учасників брейншторму не повинен вдаватися до оціночних суджень щодо ідей інших учасників. Викладачі як фасилітатори брейншторму мають спостерігати за тим, щоб учасники залишалися у просторі обговорюваної теми, не переходили на обговорення інших тем та діяв принцип: коли один говорить, інші мовчать.

Ще одним підхід до ефективного використання методики брейншторму можна назвати Модель 6-3-5 (*Markman, 2017*). Для цього поділіть студентів на команди по шість осіб і посадіть кожну команду за окремий стіл. Попросіть кожного учасника команди написати три ідеї і передати їх тому, хто сидить праворуч.

Таке переміщення зробіть п'ять разів, щоб усі учасники команди могли побачити ідеї інших, пропозиції інших та додати свої думки. Після цього запропонуйте учасникам обговорити всі ідеї разом за одним столом. Хоч цей процес займе більше часу, проте дозволить висловитися всім учасникам команди та запропонувати свої ідеї.

Посилання на додаткові ідеї щодо організації брейншторму можна знайти у переліку посилань (*Markman, 2019; Markman, 2020; Tsipursky, 2022; Gregersen, 2018; Besieux et al., 2021; Rogelberg & Kreamer, 2019*).

Симуляція

Для перевірки знань студентів викладачі можуть використовувати навчальний метод "симуляційна гра". Цей метод допомагає студентам приймати рішення в аудиторії, тестуючи варіанти рішень для ситуацій, що відбуваються в умовах реальних життєвих обставин.

За допомогою симуляційної гри у студентів випрацювується аналітичне мислення і вони краще можуть описувати результати своїх спостережень. Працюючи з кейсами за допомогою симуляційної гри студенти мають змогу показати свої сильні індивідуальні сторони та свою команду, показати спроможність і внесок, який робить кожен із них в результат команди.

Методика симуляції належить до категорії **експериментального навчання** (experiential learning). Ця методика допомагає працювати з неправильними уявленнями студентів про явища та події (*McClintock, 2000*), розвиває здатність до критичного мислення (*Kreber, 2001*) та самостійного навчання (*Hakeem, 2001*) і допомагає студентам краще зрозуміти предмет.

Метод симуляційна гра можна використовувати при різних форматах навчання: онлайн, офлайн, чи змішаний онлан / офлайн формат. Значно важливішим за формат навчання, в якому ми хочемо провести симуляційну гру, є вибір симуляційної моделі, за допомогою якої слід перевірити знання студентів. Насамперед, слід обрати симуляційну гру, яка найкраще відповідає дисципліні, яка читається студентам.

Серед форм симуляційного навчання є техніка моделювання, під час якої студенти мають змогу вчитися один в одного (*Dorn, 1989*). Навчання відбувається через активну залученість кожного учасника навчального процесу, а не пасивного слухання по лінії "викладач навчає – студент слухає".

Моделювання як симуляційну практику можна застосовувати при вивченні таких тем як економіка торгівлі та економіка бідності, розвиток та становлення бізнесу, вивченні практик сімейного життя та подружньої взаємодії (*Osmond, 1979*), міжлюдської взаємодії у соціальних науках та публічному управлінні (*Rocha, 2000*).

Якісне запровадження симуляції як навчальної методики передбачає три етапи: (I) підготовка, (II) залучення студентів, (III) підсумки.

Підготовка

На етапі підготовки симуляційного завдання важливо зрозуміти, які цілі курсу і наскільки симуляційна техніка дозволяє їх досягнути. Перш, ніж застосовувати її безпосередньо на занятті, слід зробити пробний запуск. Ефективність застосування симуляційної методики тісно корелюється з рівнем активності студентів. Через це слід зважати на кількість студентів на заняття, оскільки для кожного з них має бути своя роль і ніхто із студентів не має залишитися пасивним учасником симуляційного навчання.

Для використання симуляційної техніки також має значення приміщення, в якому вона проводитиметься. Важливо, щоб симуляційна методика поєднувалася з іншою навчальною методикою, а не була єдиною, яку застосовує викладач на занятті. Оскільки щось може піти не так, викладач має також перестрахуватися, що він робитиме у такому випадку. Для максимального залучення аудиторії корисно використовувати онлайн-ресурси, відповідну інформацію можна знайти в **табл. 2**.

Залучення студентів

Симуляційне навчання ефективне при умові, що студенти активно включені у процес навчання. Викладачі мають докласти зусилля до того, щоб усі студенти були активно включені. Активність студентів зростає за умови, коли вони перед її проведенням намагаються передбачити та пояснити результати симуляційного навчання, а також коли кожен з них обирає для себе якусь роль у процесі проведення симуляції.

Підсумки

Обговорення після проведення симуляційного навчання дозволяє студентам закріпити знання та розширити простір для можливого їх застосування. Для цього у студентів має бути достатньо часу, особистої рефлексії та групового обговорення.

Важливо, щоб викладачі підготували запитання, які допоможуть студентам зістикувати між собою симуляційну практику та навчальні цілі.

Релевантною симуляційною грою у контексті проекту Erasmus WARN з виявлення та протидії гібридним загрозам може бути кейс IT-менеджмент симуляцій: гібридна атака. "Ця симуляційна гра

навчає студентів ключовим проблемам, з якими стикаються менеджери, реагуючи на IT-кризу. Виконуючи роль технічного директора у компанії в розпал кібератаки, студенти навчатимуться визначати пріоритети та приймати обґрунтовані рішення, які посилюють збереження даних. Вони орієнтуватимуться на складнощі спілкування у швидко плинному середовищі, водночас дізнаючись про важливість готовності до кризи.

У першій частині симуляції студенти зіткнуться зі сплеском інформації, суперечливими думками та низкою подій, які вони повинні діагностувати, на які повинні реагувати та після якої мають відновитися. У другій частині симуляції студентам буде доручено написати публічну заяву про напад, а потім переглянути заяви інших учасників симуляційної гри" (**табл. 4, п. 1**).

Симуляція відмінна від гри і не передбачає, що хтось буде переможцем. Вона також відмінна від методі кейс-стаді, оскільки не передбачає можливості дивитися на проблематику ззовні та зсередини.

Один із важливих елементів симуляції (на відміну від гри чи кейс-стаді) полягає у тому, що кожен учасник повинен обрати для себе свою роль і намагається вирішити проблему через подію, в якій він приймає участь.

Переваги симуляційного навчання у тому, що студенти не лише навчаються, але особисто, через певну роль у події, здобувають свій досвід.

Симуляційна методика може також не виконати свого призначення. Це можливе принаймні з трьох причин: студенти не підготовлені, у процесі симуляції студенти захоплюються певним її елементом або акцентують увагу саме на ньому. Або ж, студенти відхиляються від навчальної цілі, передбаченої курсом.

Щоб уникнути ризику непідготовленості, можна завчасно запланувати, щоб певні ролі взяли на себе студенти, які досягнуть результату. Також не слід боятися повертати студентів до основної цілі симуляційної методики.

Зазвичай симуляційну гру найкраще проводити всередині семестру, тому що вже пройде достатньо часу для вивчення матеріалу, який викладач зможе оцінити на прикладі роботи з кейсом у симуляційній грі.

Таблиця 2. Симуляційні кейси у різних сферах

№	Автори	Назва ресурсу	Опис	Посилання
1	**2**	**3**	**4**	**5**
1	Robert D. Austin	IT Management Simulation: Cyber Attack!	Симуляція ролі технічного директора компанії в розпал кібератаки	https://hbsp.harvard.edu/product/8690-HTM-ENG
2	Центр викладання та навчання Advantexe	Симуляція ситуацій у бізнесі та втілення стратегічних ініціатив	Бізнес-симуляції: – Business Acumen / Ділова хватка – Business Leadership / Лідерство – Business Selling / Продаж бізнесу	https://www.advant-exe.com/
3	Центр наукової освіти UCAR	Осмислити науку про Землю за допомогою ігор та симуляції	Ігри та симуляції, пов'язані з погодою, кліматом, наукою про атмосферу тощо	https://scied.ucar.edu/interactive
4	Проєкт PhET Interactive Simulation в Університеті Колорадо	Інтуїтивно зрозуміле середовище, схоже на гру, в якому студенти вчаться, досліджують, роблять відкриття	Симулятори PhET засновані на освітніх дослідженнях в галузі: – Physics / Фізика – Chemistry / Хімія – Math / Математика – Earth Science / Наука про Землю – Biology / Біологія	https://phet.colorado.edu/

Продовження Таблиці 2

1	2	3	4	5
5	BBC	Сирійська подорож: виберіть власний шлях втечі	Якби ви тікали з Сирії, щоб ви зробили для своєї родини? Зрозумійте справжні дилеми, з якими стикаються біженці	https://www.bbc.com/news/world-middle-east-32057601
6	Розробка McKinney для Urban Ministries of Durham (США)	SPENT – онлайн-гра про бідність і безпритульність	Гравці мають приймати складні рішення в умовах бідності, щоб прожити один місяць на 1000 доларів, та часто змушені вибирати між однаково поганими варіантами (вибір між оплатою електроенергії та здоровою їжею) тощо	http://playspent.org/html/
7	Harvard Business Publishing	Помістити студентів прямо в контекст реалістичних бізнес-сценаріїв, де вони повинні застосовувати концепції, яким навчилися, щоб приймати рішення під тиском	Моделювання у різних дисциплінах: – Accounting / Бухгалтерський облік – Economics / Економіка – Entrepreneurship / Підприємництво – Finance / Фінанси – Management / Менеджмент – Information Technology / Інформаційні технології – Marketing / Маркетинг – Strategy / Стратегія тощо	https://hbsp.harvard.edu/simulations

Симуляції можуть працювати як індивідуальні чи групові проєкти, незалежно від розміру класу. Однак, щоб керувати часом уроку більш ефективно, слід розглянути можливість проведення симуляційної вправи як групового проєкту, у кожній групі не більше чотирьох учасників.

Джерела посилань

Al-Samarraie, H., Hurmuzan, S. (2018). A review of brainstorming techniques in higher education. Thinking Skills and Creativity, 27, 78–91. doi: https://doi.org/10.1016/j.tsc.2017.12.002

Besieux, T., Edmondson, A. C., de Vries, F. (2021). How to Overcome Your Fear of Speaking Up in Meetings. Harvard Business Review. Available at: https://hbr.org/2021/06/how-to-overcome-your-fear-of-speaking-up-in-meetings

Dorn, D. S. (1989). Simulation Games: One More Tool on the Pedagogical Shelf. Teaching Sociology, 17 (1), 10–18. doi: https://doi.org/10.2307/1317920

Gogus, A. (2012). Brainstorming and learning. Encyclopedia of the sciences of learning. Springer, 484–488. doi: https://doi.org/10.1007/978-1-4419-1428-6_491

Gregersen, H. (2018). Better Brainstorming. Harvard Business Review. Available at: https://hbr.org/2018/03/better-brainstorming

Hakeem, S. A. (2001). Effect of Experiential Learning in Business Statistics. Journal of Education for Business, 77 (2), 95–98. doi: https://doi.org/10.1080/08832320109599056

Kreber, C. (2001). Learning Experientially through Case Studies? A Conceptual Analysis. Teaching in Higher Education, 6 (2), 217–228. doi: https://doi.org/10.1080/13562510120045203

Markman, A. (2017). Your Team Is Brainstorming All Wrong. Harvard Business Review. Available at: https://hbr.org/2017/05/your-team-is-brainstorming-all-wrong

Markman, A. (2019). Bring Your Brain to Work: Using Cognitive Science to Get a Job, Do it Well, and Advance Your Career. Harvard Business Press.

Markman, A. (2020). How to Brainstorm – Remotely. Harvard Business Review. Available at: https://hbr.org/2020/07/how-to-brainstorm-remotely

McClintock, C. (2000). Creating Communities of Practice for Experiential Learning in Policy Studies. Social Change, Public Policy, and Community Collaborations, 33–51. doi: https://doi.org/10.1007/978-1-4615-4653-5_4

Osmond, M. W. (1979). The Use of Simulation Games in Teaching Family Sociology. The Family Coordinator, 28 (2), 205–216. doi: https://doi.org/10.2307/581676

Rocha, C. J. (2000). Evaluating Experiential Teaching Methods in a Policy Practice Course. Journal of Social Work Education, 36 (1), 53–63. doi: https://doi.org/10.1080/10437797.2000.10778989

Rogelberg, S., Kreamer L. (2019). The Case for More Silence in Meetings. Harvard Business Review. Available at: https://hbr.org/2019/06/the-case-for-more-silence-in-meetings

Roth, B. (2015). The achievement habit: Stop wishing, start doing, and take command of your life. New York: HarperCollins Publishing.

Tsipursky, G. (2022). Why Virtual Brainstorming Is Better for Innovation. Harvard Business Review. Available at: https://hbr.org/2022/02/why-virtual-brainstorming-is-better-for-innovation?utm_medium=email&utm_source=newsletter_weekly&utm_campaign=ascend_activesubs&deliveryName=DM185859

Кнапп, Дж., Зерацкі, Дж., Ковіц, Б. (2016). Спринт: Вирішуйте складні завдання і тестуйте нові ідеї за п'ять днів. Київ: ТАО.

6. ВАРГЕЙМІНГ: ВОЄННІ ІГРИ

Світлана Гришко[1]
Олександр Котуков[2]
[1]Харківський національний університет радіоелектроніки
[2]Харківський національний університет імені В. Н. Каразіна

Будь-яка спроба проаналізувати майбутнє спирається **на судження про невизначеність**. Особливо це стосується війни, яка є хаотичною і залежить від випадковості. Тому у сфері військового аналізу напрацьовані різні підходи до прийняття рішень в умовах складних та невизначених загроз.

Ці практики набувають актуальності **для цивільних спеціалістів в умовах гібридних загроз**, де розмивається межа між миром та війною, а зловмисник використовує військові принципи підходи і навіть інструменти в невійськових доменах для створення невизначеності та неідентифікованості. Але використання військових інструментів аналізу у цивільному освітньому процесі вимагає розуміння області та специфіки їх застосування.

Висока невизначеність військових конфліктів виникає через:

1) відсутність реальних даних для створення кількісних моделей, які б забезпечували статистичну достовірність;

2) неможливості кількісно оцінити такі ключові якісні чинники, як моральний дух і підготовка військ (*Cancian et al., 2023; с. 24*).

Ці проблеми характерні й для аналізу гібридних впливів. За цей час напрацьовані різні способи аналізу військових конфліктів, які спрямовані на зменшення вказаних типів невизначеностей:

1) **неструктуровані судження:** формування уявлення про хід подій на основі розуміння потужності збройних сил та за аналогією з епізодами воєнної історії;

2) **слабо структуровані судження:** прості кількісні порівняння (наприклад, чисельності збройних сил), яким бракує оцінки динамічної взаємодії;

3) **структуровані судження:** враховують комплекс критичних змінних, як-от:

– **планування місії** – моделювання параметрів METT-TC: Mission, Enemy, Terrain, Troops, Time, Civilians – Місія, Ворог, Місцевість, Війська, Час, Цивільні;

– **чиста оцінка** – це оцінка військових балансів за критичними напрямками;

4) **кількісні моделі** – це математичне представлення системи, як, наприклад, моделі **аналізу кампаній**: двосторонні моделі TACWAR та CEM для імітації бойових дій з розрахунком виснаження, які використовувались до 1990-х років; сучасні моделі військових кампаній (як JICM і STORM) тощо.

При аналізі у військовій справі історично існувало протиріччя між кількісним моделюванням та якісними судженнями. В ідеалі, аналіз конфлікту повинен поєднувати строгість і прозорість моделювання аналізу кампанії з людським фактором прийняття рішень. **Варгеймінг пропонує один з інструментів для поєднання цих двох підходів.** Саме ця важлива характеристика привертає увагу до воєнних ігор як до способу набуття навичок захисту в умовах гібридних загроз.

Варгеймінг (wargaming) не має єдиного загальноприйнятого визначення, наступні підходи якого відображають основні характеристики цієї практики:

– симуляція воєнних дій із використанням певних правил, даних, методів і процедур і зосереджена на рішеннях гравців, які впливають на послідовність подій (*NATO, 2022*); на **рис. 2** в ілюстративній формі представлена проблематика варгеймінгу, яку досліджують спеціалісти НАТО;

– модель воєнних дій, яка не залучає реальні сили, де на перебіг подій впливають рішення, прийняті під час цих подій гравцями, що представляють протиборчі сторони (*Perla, 1990*);

– техніка прийняття рішень на основі створення структурованого середовища, де можна вільно експериментувати, ризикувати

та здійснювати помилки, не страхуючись від негативних наслідків, щоб дослідити, що працює (перемога / успіх), а що ні (програш / невдача), як правило, за відносно низьку вартість (*DCDC, 2017; p. 5*);

– ігри, в яких люди приймають рішення в контексті конкуренції, конфлікту (*U.S. Naval War College, 2020*);

– структуровані розмови між експертами для прийняття рішень (*Vatne et al., 2022; p. 299*).

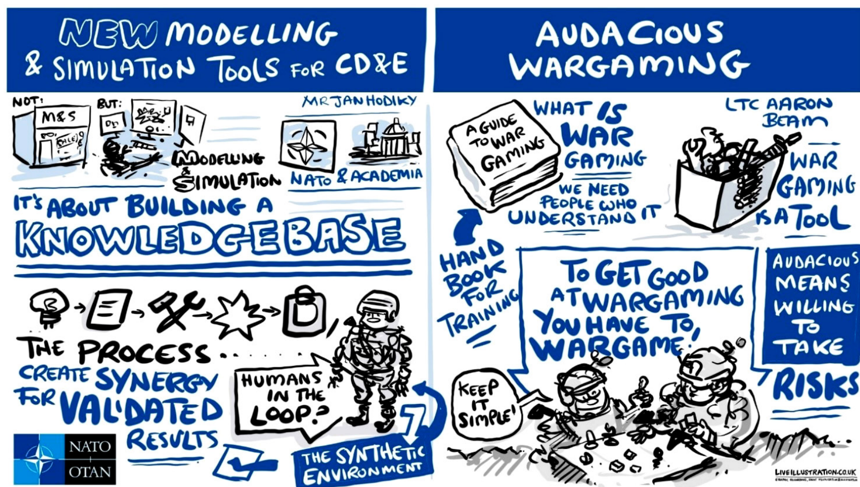


Рис. 2. Ілюстрація проблематики варгеймінгу, яка обговорювалась на міжнародній конференції CD&E (*NATO, 2022*), та розміщена на офіційній сторінці цієї конференції *https://www.act.nato.int/cde-conf*

Важливо, що варгеймінг стосується **конфліктних ситуацій**, де люди змагаються у **різних ролях**, приймаючи свої рішення як реагування на рішення інших гравців. З точки зору навчання протидії гібридним загрозам, важливо, що такі ігри підходять для **занурення учасників у середовище**, описане сценарієм, де вони піддаються різноманітним динамічним викликам і залежать від рішень інших учасників.

Організаційно варгеймінг – це процес креативного змагання, який подається у структурованому форматі та зазвичай здійснюється під керівництвом суддів. Він відбувається як певна динаміка подій, які створюються під впливом гравців. Поняття, які формують лексикон варгеймінгу, представлені в Додатку А.

Дизайн варгеймінгу складають такі елементи:

– мета і завдання: мають важливе значення для того, щоб проблема, яку необхідно розв'язати, була належним чином сформульована;

– дані та джерела: для створення установок та сценарію потрібна інформація, крім того, для моделювання потрібні кількісні параметри та дані;

– установки та сценарій, які забезпечують захоплююче середовище, у якому відбувається вся гра;

– допоміжний персонал та предметні спеціалісти – експерти, які допомагають створити гру та допомагають під час її проведення;

– гравці – діючі особи, які беруть на себе певні ролі, їх рішення створюють динаміку гри; кількість гравців може коливатися від одного до тисячі. Зазвичай вони організовані у групи, розмір і форма яких може значно змінюватися, має місце є кольорове кодування таких груп (див. додаток А);

– координатори (судді) – команда, що піклується про досягнення цілей гри, підтримує занурення гравців, виносить рішення (судить), модерує процес;

– симуляція, яка відбувається на основі створених установок, правил, процедур та критеріїв;

– аналіз – заснований на даних, зібраних у грі, дозволяє зрозуміти створений під час гри наратив, в основі якого спільний досвід гравців та уроки, які були отримані.

Складність елементів буде різною, але всі вони зазвичай присутні у варгеймінгу.

Воєнні ігри мають довгу історію у військовому аналізі та використовуються як педагогічні і дослідницькі інструменти в університетах, аналітичних центрах та урядових установах для вивчення питань безпеки – від кризової стабільності до регіональних конфліктів. В залежності від мети, воєнні ігри бувають (*Cancian et al., 2023; p. 26*):

1) **експериментальні** – мають на меті краще зрозуміти процес прийняття рішень людиною у конкретному контексті. Через маніпулювання ключовими змінними і запис дискусій, така гра дозволяє виявити варіанти розвитку подій;

2) **навчальні** – мають на меті сприяти підготовці лідерів до прийняття рішень на війні через моделювання вибору у складних умовах, при цьому виділяють:

– ігри, орієнтовані на "трансформацію себе", які надають військовим командирам **досвід** прийняття рішень;

– ігри, орієнтовані на поточні операції, які зосереджені на актуальній **інформації**, необхідній для прийняття рішень у даній ситуації;

3) **аналітичні** воєнні ігри, спрямовані на аналіз військових проблем у контексті всього спектру PMESII – доменів[1]. Для цього створюється аналітична архітектура, в якій будуються моделі на основі фактичних даних, потім розробляється дизайн гри, що перевіряється експертами у цій галузі; ця гра потім ітеративно розігрується невеликою групою людей для полегшення аналізу. Такий аналіз передбачає велику кількість ігрових ітерацій, варіативність сценаріїв і прийняття рішень на основі науково обґрунтованих правил.

Повний цикл військових досліджень об'єднують **воєнні ігри** ("маневри на карті"), **аналіз кампаній і військові навчання** ("польові маневри") для розуміння сценаріїв розгортання сучасної війни. Варгеймінг порушує питання, які потім досліджуються за допомогою військових навчань і математичного аналізу.

Застереженням до використання воєнних ігор є дотримання області використання: не слід плутати варгеймінг з конструктивним моделюванням – якщо варгеймінг був призначений для навчання учасників, але використовується як основа для аналізу, це призводить до марних зусиль і хибних висновків. Варгеймінг дозволяє моделям взаємодіяти в інтелектуальний спосіб. Конкретні події,

---

[1] PMESII – політичний, військовий, економічний, соціальний, інформаційний, інфраструктурний спектр. https://warn-erasmus.eu/glossary/pmesii/

з яких генеруються сценарії, є результатом інтелектуального прийняття рішень людьми-гравцями.

Кількісні результати створюють основу для якісних суджень про вплив однієї сфери на іншу.

При моделюванні варгеймінгу важливо **забезпечити наступні умови**:

1) збалансувати ступінь спрощення та кількість областей моделювання (наприклад, наземна, повітряна кампанії) та типів бойових дій;

2) визначити адекватні правила взаємодії, розподілу ресурсів та прийняття рішень, збалансувати складність та точність моделі;

3) сформувати:

– змінні – умови, які можуть вплинути на аналіз;

– сценарії – набори обґрунтованих припущень для кожної змінної;

4) забезпечити достовірність моделі: позначити, які області вимагають точності, а які можуть розглядатися абстрактно;

5) врахувати умову повноти моделі, включивши до неї всі критично важливі елементи: гра доречна лише тоді, коли обрані частини є єдиними значущими частинами конфлікту (наприклад, ракети класу "земля-повітря" є критично важливим елементом сучасного повітряного бою).

Мета гри – це не спроба дослідити всі можливі результати (це нереально), а спосіб оцінити основні лінії гри, які є результатом розумного прийняття рішень. Кожна ітерація дозволяє дослідити деякі з найбільш вірогідних варіантів розвитку подій, але одна ітерація не може проілюструвати загальні контури проблем. Повторне програвання сценарію з використанням різних стратегій необхідне, щоб недопустити помилкової орієнтації на стратегію, отриману з одного сценарію. **Ітерації виконують важливу роль** для створення висновків:

– ітерація у різних сценаріях з різними припущеннями щодо ключових змінних дозволяє провести аналіз чутливості;

– проводячи кілька ітерацій з одним сценарієм, а потім змінюючи сценарій, можна зробити висновки про важливість і вплив кожної зміни змінної.

Вибір **змінних** має відображати мету такої гри. Змінні повинні бути одночасно **невизначеними** і такими, що можуть мати **значний вплив** на результат. Вибір може ґрунтуватися на літературі або на уявленнях, отриманих під час гри (виявлення "невідомих невідомих").

Елемент **випадковості** (несподівана подія, шанс) досягається завдяки генератору випадкових чисел (гральні кубики, таблиці з інструментами, картки з подіями).

Активні, мислячі опоненти та елемент випадковості є основними засобами введення **невизначеності** у гру, однак можуть використовуватися інші методи:

– таємні рухи, поки розвідка їх не виявить;

– незрозумілі або невизначені цілі та наміри (включаючи цілі союзників);

– випадкові чинники сценарію (негода, технічна поломка, увага ЗМІ тощо);

– зміна послідовності гри, що може дозволити одній стороні зробити щось потайки або потрапити у процес прийняття рішень противника тощо.

Конкретний результат кожної ітерації не може передбачити майбутнє, але сам процес воєнних ігор є необхідним для аналізу конфлікту. **Будьте обережними**, граючи у варгеймінг, щоб не робити тверджень, які виходять за межі їх сфери застосування, і не плутати висновки воєнної гри з висновками їх моделювання.

Організація варгеймінгу може бути здійснена різними способами (*DCDC, 2017, p. 39–40; Vatne et al., 2022, p. 300*), основні з них представлені в **табл. 3**.

Варгеймінги є повторюваними і мають циклічний життєвий цикл:

1) проєктування; розробка;

2) проведення гри;

3) оцінка результатів та уточнення моделі.

Кожен етап вимагає ретельної підготовки (*DCDC, 2017, p. 51–60*).

Приклад організації варгеймінгу для спеціальності "Публічне управління та адміністрування" наведений у Додатку Б. Посилання на приклади організації варгеймінгу представлені в **табл. 4**.

Таблиця 3. Організаційні форми варгеймінгів

Форма	**Опис**
Ігри-семінари	Модеровані дискусії між людьми у спільному контексті / сценарії. Зазвичай мають вільну форму, носять дослідницькій характер, мають справу з відкритою інформацією. Гравців занурюють у контекст, просять приймати рішення, а потім обговорюють наслідки. Висновки ("Судові рішення") зазвичай є менш жорстким, але достатнім для просування перебігу подій. Винесення рішення може здійснюватися суддею або за консенсусом між гравцями. Зазвичай проводяться у малих групах. На відміну від звичайного семінару містить причинно-наслідкову взаємодію, змагальність та висновки про наслідки конкретних дій
Матричні ігри	Відбуваються за розподілом ролей та використовують формальні правила суддівства. Від гравців вимагається надати кілька конкретних аргументів на користь запропонованої дії, яка обмежена фантазією гравця або її реалізацією. Потім інші гравці можуть наводити контраргументи. Наступне коротке обговорення веде безпосередньо до результату винесення рішення. Дебати обмежені за часом, щоб дозволити кілька дій і протидій у грі. Тож учасники змушені жити з наслідками своїх рішень у наступних ітераціях. Модерують гру координатори / судді, які оцінюють аргументи "за" і "проти", та приймають рішення про ймовірність успіху курсу дій. Результат визначається киданням кубиків. Матричні ігри підходять для дослідження різних перебігів подій у контексті одного сценарію
Кригшпіль (Kriegsspiel)	Більш формальні воєнні ігри з підвищеним рівнем деталізації та суворості. Мають більш реалістичне уявлення про конфлікт із більш детальними сценаріями та представленням середовища

Таблиця 4. Опис прикладів організації варгеймінгу

№	Кейс	Опис	Посилання
1	Китайське вторгнення на Тайвань у 2026 році	Розробник: Центр стратегічних і міжнародних досліджень (CSIS), США Гра проведена у січні 2023 Чи вдасться китайське вторгнення? Які змінні впливають на результат? Якою буде вартість для обох сторін?	Cancian et al., 2023; p.40 – 160
2	Балтійський виклик	Розробник: Спільнота з дослідження військових операцій (MORS), USA; Tom Mouat (PAXsims). Гра проведена 17–20 жовтня 2016 Позиціонування сил НАТО / росії в Балтійському морі	http://www.mapsymbs.com/BalticChallenge.pdf
3	Kazhdyy Gorod	Розробник: Tom Mouat (PAXsims) Матрична гра "про місто колишньої радянської республіки Belaria на кордоні з росією, "січневу революцію" та протести"	http://mapsymbs.com/KazhdyyGorodSeriousMatrixGame.pdf

Джерела посилань

About wargaming. What is a war game? (2020). U.S. Naval War College. Available at: https://usnwc.edu/Research-and-Wargaming/Wargaming/About-Wargaming

Cancian, M., Cancian, M., Heginbotham E. (2023). The First Battle of the Next War. Wargaming a Chinese Invasion of Taiwan. A Report of the CSIS International Security Program. CSIS, 165. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/230109_Cancian_FirstBattle_NextWar.pdf

Perla, P. (1990). The art of wargaming. A guide for professionals and hobbyists. United States Naval Institute.

The Development, Concepts and Doctrine Centre (2017). Wargaming Handbook. DCDC. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

Vatne, D., Guttelvik, M., Hennum, A. C., Malerud, S. (2022). Wargaming for the Purpose of Knowledge Development: Lessons Learned from Studying Allied Courses Of Action. Scandinavian Journal of Military Studies, 5 (1), 297–308. doi: https://doi.org/10.31374/sjms.122

Wargaming the Future at the CD&E Conference. NATO. Available at: https://www.act.nato.int/cde-conf/cde-wargaming-future

8. ГРА В ДИЛЕМУ

Світлана Гришко[1]
Марія Головянко[1]
[1]Харківський національний університет радіоелектроніки

Для формування компетентностей з протидії гібридним загрозам можна використати підходи та методи антикризового управління.

Це пояснюється тим, що під час антикризового управління, так само як і в умовах гібридних впливів, відбувається прийняття "**складних рішень**", характеристиками яких є (*França & Borges, 2020*):

– стратегічний характер та високий рівень прийняття рішень, у результаті чого рішення піддаються впливам політичних міркувань, і тому стикаються з необхідністю узгодження розбіжних інтересів, а також вимагають сприйняття втручань населення (занепокоєння, недовіри, негативного впливу на політичну репутацію тощо);

– важливість: такі рішення впливають на розподіл важливих ресурсів та мають вирішальне значення для забезпечення життєдіяльності спільноти;

– ситуативність та контекстуальність (через унікальну природу кожної проблеми);

– когнітивна складність та високий рівень стресу, зокрема – й через ситуації "подвійного зв'язування" (double bind situations), коли менеджер отримує дві або більше суперечливих порад, одна порада з яких заперечує іншу;

– складні обставини – це динамічні та мінливі умови, невизначеність, неоднозначність, високі ставки, значні наслідки помилок, обмеження часу;

– міждисциплінарний характер, що ускладнює спільну ситуаційну обізнаність.

Велика частина невдач в управлінні кризою є результатом помилкового спільного усвідомлення ситуації (*DRIVER+ project, 2017; с. 12*). Особливо у тих випадках, коли вирішення проблеми має два та навіть більше варіантів, але жоден з них не є однозначно прийнятним чи кращим. Це вимагає зважування різних типів потенційних катастрофічних впливів, які необхідно пом'якшити (тобто **визначення пріоритетів**). Тому прийняття рішень в антикризовому управлінні часто стосується вирішення дилем.

Дилема – це ситуація, коли необхідно зробити важкий вибір між двома або більше альтернативами, які однаково небажані (*Oxford Reference*)

В умовах гібридних загроз, так само як і в антикризовому менеджменті, виникають дилеми. Коли **цінності людини входять у конфлікт**, створюються етичні, або ще гірше – моральні дилеми.

Етична дилема – це ситуація, в якій порушені правила життя конкретної особистості; вона зачіпає коло етичних питань: добро і зло, свобода та відповідальність, сенс життя, совість, обов'язок, щастя тощо

Найчастіше доводиться вибирати між тим, що правильно (з погляду моралі), але невигідні людині, – і тим, що погано для інших, але приносить особисту вигоду. У соціальних відносинах етична дилема – це, наприклад, безпека споживачів, права та дискримінація, професійна етика, корупція тощо.

Моральна (соціальна) дилема – це ситуація, в якій порушені норми моралі, тобто прийняті у суспільстві правила поведінки

Це – одна з найважчих ситуацій, в яку тільки можна потрапити. Необхідно вибрати один із взаємовиключних варіантів, причому обидва не принесуть нічого хорошого. Вирішення мораль-

них дилем розглядається у курсах логіки, конфліктології, психології, теорії ігор тощо. Існують загальновідомі постановки завдань: "дилема ув’язненого", "дилема секретаря", "дилема самаритянина", "дилема стрілочника" та інші. Пандемія COVID-19 породила низку моральних дилем. Наприклад, дослідження *Everett et al.* (*2021*) представлене в Nature Human Behavior, вивчає – чи повинні лідери віддавати перевагу власним громадянам над людьми в інших країнах під час розподілу обмежених ресурсів.

Про дилеми люди зазвичай вважають за краще не замислюватися. А у тих, хто розмірковує, гіпотетичний вибір може і не збігтися з реальним, якщо виникне справжня дилема. Але саме перед такими дилемами ставлять гібридні зловмисники звичайних непідготовлених громадян. Пошук виходу з ситуації, яка не має хороших рішень вимагає **внутрішньої роботи людини із собою**.

Рішення "нерозв'язних" дилем потребує не лише певного когнітивного рівня, але й розвинутого морального мислення. Моральні міркування людини розвиваються протягом всього її життя. І так само, як і когнітивні – вони можуть бути здобуті під час навчання. Визнання та знання того, як керувати етичними та моральними дилемами, можна вважати **етичною навичкою**.

Багатообіцяючим способом навчити приймати рішення в умовах дилем є створення **спільного ігрового середовища**, у якому відбувається симуляція складної ситуації і люди співпрацюють для її вирішення через прийняття рішень. В іграх з дилемами гравці занурюються у сценарій, який базується на гострій, всеосяжній, неоднозначній проблемі, яку не вийде класифікувати як одновимірну чи суто технічну. Гра в дилему дозволяє змоделювати будову (структуру) ситуаційної обізнаності під час кризи та напрацювати навички контролю над складною ситуацією в міру її розвитку, що є однією з найскладніших частин в урегулюванні кризи.

Ситуаційна обізнаність (situation awareness, SA) – це сприйняття елементів навколишнього середовища в обсязі часу і простору, розуміння її значення і прогнозування їх стану в найближчому майбутньому (*Endsley, 1995; c. 36*)

Підтримувати точну спільну операційну картину та досягти спільної ситуаційної обізнаності значно складніше, ніж отримати індивідуальну ситуаційну обізнаність. Отже, формат командної гри є ефективним і з точки зору тренування навичок співпраці та взаємодії.

Розробка ігри-дилеми – не проста навчальна задача. Тут може стати у нагоді **досвід** дослідницької організації **TNO** (https://www.tno.nl/en/), яка, серед інших завдань, вивчає та запроваджує комплексні освітні підходи для набуття компетентності у прийнятті складних рішень. Низка проєктів, в яких спеціалісти TNO взяли участь, спрямовані на конструювання навчального процесу через ігри-дилеми. Результатом проєкту "GATE3 Pilot Safety" (Нідерланди, 2009–2012 рр.) стала "Гра мерів", The Mayor Game (*Stubbé et al., 2014*). Вона вчить приймати політичні рішення на високому рівні і використовується для того, щоб навчити нових мерів управлінню кризовими ситуаціями. Більшість мерів Нідерландів пройшли навчання за сценаріями цієї гри. Підхід узагальнено у потужному консорціумі більш ніж 30-ти команд в рамках проєкту DRIVER+ (https://www.driver-project.eu/).

При конструюванні ігор-дилем, TNO спирається на ідею **експериментального навчання**. Згідно з нею, учасники повинні активно розвивати свої навички, щоб самостійно набути тактичних знань і вмінь. Навчання має відбуватись на досвіді. Принципи, які підтримують цю ідею, мають бути дотримані у дизайні ігри-дилеми:

– "спочатку практика – потім теорія": теоретичний зміст не надається заздалегідь, а здобувається під час вирішення реалістичних проблем; окрім того, що досвід робить людей сприйнятливими до теорії, це одночасно тренує розв'язання проблем в абсолютно нових ситуаціях;

– "рефлексія обов'язкова" – набутий досвід необхідно концептуалізувати та закріпити після кожного сценарію; цей процес об'єднує знання та успішні стратегії застосування цих знань, які є типовими компетентностями експерта.

– "короткий цикл" – що дозволяє швидко повторювати короткі вправи і зіткнутися з якомога більшою кількістю різних налаштувань протягом визначеного часу (тренування має відбуватись не довше одного дня).

– "поступове збільшення складності" – замість одного великого сценарію слід програти серію сценаріїв, складність яких поступово зростає.

– "виклик": навчальні проблеми мають бути досить складними, щоб кинути виклик, бо навчання важким шляхом – це найшвидший шлях до кваліфікації.

– "тренування частини завдання": гра має бути спрямована лише на прийняття рішень і відділена від процедурного контексту.

Дизайн гри з дилемою зазвичай складається з елементів, представлених у **табл. 5**.

Таблиця 5. Складові ігри-дилеми

Складова	**Характеристика**
1	**2**
Проблема	Має бути всеосяжною, неоднозначною, не одновимірною і не технічною, складною (складатися з багатьох дилем) і вимагати прийняття стратегічного рішення. Приклади "поганих проблем", які підходять для гри в дилеми: – (потенційний) зовнішній конфлікт (наприклад, гібридна війна); – великомасштабне лихо або природна криза (наприклад, пандемія); – геополітична та економічна конкуренція (наприклад, Арктика); – внутрішня дестабілізація або поляризація (наприклад, тероризм)
Роль (Актор)	Можуть грати багато гравців (часто – у командах з двох осіб, щоб стимулювати взаємне обговорення). Усім гравцям призначається одна роль, яка є фіксованою для всієї гри. Актор та його повноваження пов›язані з проблемою. Наприклад, у разі конфлікту між країнами актором можна вибрати генерального секретаря НАТО, а якщо країну може дестабілізувати терористичний акт, актором можна вибрати прем'єр-міністра країни

Продовження Таблиці 5

1	2
Дилеми	Дилеми мають задовольняти таким вимогам: – двійковість – повинні мати лише два варіанти відповіді: "так" чи "ні"; – реальність – варіанти (так чи ні) повинні мати недоліки (подвійне зв'язування); – реалістичність для цільової групи: багато рішень, які ми вважаємо дилемами, для практиків є безглуздими, потрібно це перевірити; – незалежність – кожна дилема має бути незалежною у серії дилем, не впливати на загальний хід сценарію, щоб уникнути зайвої деталізації. Приклади дилем в умовах гібридних загроз: – пріоритетність (стимулювання бізнесу vs. соціальне забезпечення); – короткотермінові ефекти та довгострокові наслідки; – зіткнення інтересів (прибутки vs. безпека у справі Huawei); – моральні проблеми (пожертвувати селом для порятунку міста); – юридичні проблеми (конфіденційність vs. безпека проти злочинів); – відоме проти невідомого (поточна чи принципово нова технологія); – індивідуальні інтереси проти спільних (фінансова криза ЄС); – протистояння чи пом›якшення наслідків (викриття vs. дипломатія); – дія проти роздумів (швидко реагування COVID-19 vs. вичікувати); – зміна проти стабільності та безперервності (наприклад, Brexit); – прагматичне проти ідеологічного (китайські інвестиції vs. Неприйняття порушення прав людини в Китаї)
Передісторія	Пояснює поточну ситуацію та містить інформацію про: – відповідних акторів (державні та недержавні);

Продовження Таблиці 5

1	2
	– кілька важливих подій (минулих, поточних, запланованих); – географічне та часопросторове середовище; – деякі виклики, з якими доводиться стикатися акторам. Має бути обмеженою 1 сторінкою. Зайві деталі не потрібні, лише магістральні лінії. Гравці можуть самостійно додати вмісту з фактичної ситуації. Брифінг краще представити колективно, з деякими ілюстраціями
Дорадчі ролі	Радники надають аргументи, щоб мотивувати "так" чи "ні" рішення. Визначають до 10 радників і обирають для кожної дилеми відповідних. Поради (кількість радників) для кожної дилеми мають бути збалансовані: мають бути порадники, які кажуть "так", і порадники, які кажуть "ні", бажано майже у рівній кількості. Але якщо є один дійсно вагомий аргумент, можна вирішити, щоб інші радники заперечували цей аргумент, і таким чином створили баланс у якості замість кількості. Кожна порада має ґрунтуватися на 1 або 2 переконливих аргументах. Поради слід формулювати дуже стисло; не варто згадувати всі деталі і бути дипломатичними. Краще – чорно-білі точні поради замість сірих. Радники мають представляти всі інтереси, думки та/або організації. При визначенні радників рекомендується вибирати різні рівні. Наприклад, усі – на рівні політики, або всі на рівні міністра тощо. Дорадчі ролі, які часто використовуються та змішуються в іграх: – національні департаменти (економічні, закордонні справи, МО); – національні агентства (розвідка, охорони здоров'я); – міжнародні організації (НАТО, ЄС, ВООЗ); – глави держав; – генеральні директори великого бізнесу тощо

Продовження Таблиці 5

1	**2**
Зворотній зв'язок	Для деяких ігор можна надавати заздалегідь приготовлені відгуки про прийняті рішення. Це необов›язково. Такі відгуки мають форму журнальної статті. Вони містять опис того, що сталось, якщо прийнято рішення "так" (або – що сталось при рішенні "на") та забезпечать перехід до наступних подій
Рефлексія	Основна дискусія відбувається після гри в дилему. Модератор дозволяє всім запропонувати свій вибір і, що важливо, свою мотивацію та аргументи. Обговорення займає 30-45 хвилин. Зручно використовувати інструменти підтримки, такі як система електронного голосування, яка забезпечує швидкий огляд відмінностей у відповідях. Це також полегшує анонімну реєстрацію результатів, що може бути корисним для виявлення спільних тем під час багаторазової гри в дилему. Журнал також є корисним для оцінки дилем. Іноді здається, що дилема не є справжньою, що може відображатися в одностайних балах

Фахівцями TNO були розроблені **рекомендації для конструювання** ігор-дилем, які не обмежують формат гри (можна відтворювати у паперовому форматі та у програмній версії), а також не висувають особливих вимог до ведучого (достатньо обмеженого навчання).

Але рекомендації містять такі обмеження:

– ігри слід запускати на дуже короткий проміжок часу – до 90 хвилин (включно з обговоренням);

– гравці мають отримуватимуть поради щодо будь-якої дилеми, зазвичай це 4–5 різних порад з різних точок зору;

– кожна гра складається з набору у 6–8 дилем.

Перш ніж використовувати гру в дилеми у реальній аудиторії, рекомендується провести попереднє тестування: переглянути

всі дилеми та консультативні аргументи (бажано експертами), за необхідності – доопрацювати чи перефразувати їх; а також – перевірити час, необхідний для повної гри.

Також важливо врахувати, що гра має на мети надати навички прийняття рішень у прискореному режимі. Тому не бажано, щоб учні витрачали час на ознайомлення з інструментами такої гри. Отже, важливою вимогою до конструювання гри-дилеми є зручність використання. Особи, які приймають стратегічні рішення, мають використовувати гру без навчання та, бажано, без пояснень – гра повинна мати простий інтуїтивно-зрозумілий інтерфейс.

Приклад розробки та результати тестування гри-дилеми "Dilemma: Flooding game" ("Гра у повінь") презентовані у звіті *DRIVER+ project (2017), p.22–32*, більше прикладів тестування з описом різних реалістичних сценаріїв дилем – на офіційному сайті проєкту у розділі Trials (https://www.driver-project.eu/trials/).

Джерела посилань

Dilemma. Oxford Reference. Available at: https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095718683

Endsley, M. R. (1995). Measurement of Situation Awareness in Dynamic Systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37 (1), 65–84. doi: https://doi.org/10.1518/001872095779049499

Everett, J. A. C., Colombatto, C., Awad, E., Boggio, P., Bos, B., Brady, W. J. et al. (2021). Moral dilemmas and trust in leaders during a global health crisis. Nature Human Behaviour, 5 (8), 1074–1088. doi: https://doi.org/10.1038/s41562-021-01156-y

França, J. B. S., Borges, M. R. S. (2020). Systematizing the impacts projection of complex decisions in work groups. SN Applied Sciences, 2 (7). doi: https://doi.org/10.1007/s42452-020-3086-4

Method and Tool for Training Decision-Making Context -D934.12 (2017). DRIVER+ project. Available at: https://www.driver-project.eu/wp-content/uploads/2018/02/DRIVER-_D934.12_Method-and-tool-for-training-decision-making-context.pdf

Stubbé, H., Ven, J. G. M., van de Hrehovcsik, M. (2014). Games for top civil servants: An integrated approach. Cases on the Societal Effects of Persuasive Games. IGI Global, 32–50. doi: https://doi.org/10.4018/978-1-4666-6206-3.ch003

8. НАВЧАННЯ СТІЙКОСТІ

Марія Головянко[1]
Світлана Гришко[1]
[1]Харківський національний університет радіоелектроніки

8.1. Формування стійкості до переконання: теорія щеплення

Існує хибна думка, що дискусія навколо проблемного питання сама по собі приносить користь. Думка є хибною, бо часто суперечка лише зміцнює учасників у власній думці та в цінностях.

Викладання дисциплін з протидії гібридним загрозам має враховувати **соціальну теорію щеплення**, згідно якої власні переконання чи ставлення стають більш стійкими під впливом "ослаблених" контраргументів (*Compton, 2013*).

Слабкі контраргументи викликають опір в адресата, що дозволяє йому зберегти свої переконання перед обличчям майбутньої, сильнішої атаки. Після впливу **слабких контраргументів** (наприклад, які були поєднані зі спростуваннями), одержувач буде шукати підтверджуючу інформацію, щоб **ще більше посилити свою позицію**. Через це ставлення чи переконання стають стійкими до сильнішої атаки.

Соціальна теорія щеплення (теорія інокуляції) була розроблена за аналогією з медичною теорією формування імунітету через щеплення (**табл. 8**).

Ідея **вакцини від промивання мізків** ("vaccine for brainwash") передбачає наступне: замість того, щоб бомбардувати людей підтверджуючими фактами (аргументами), слід завчасно надати "ослаблену" дозу переконливого маніпулятивного контраргументу.

Таблиця 6. Теорія щеплення: порівняння біологічної та соціальної вакцинації

Елементи імунного захисту	**Біологічне середовище**	**Соціальне середовище**
1	**2**	**3**
Науковий бекграунд	Імунологія (*Луї Пастер, 19 ст.*)	Теорія інокуляції (*McGuire, 1961*)
Об'єкт захисту	Живі організми	Переконання та ставлення людей
Загроза (чужорідний агент)	Інфекційний агент (патоген): молекули інших організмів, мікробні клітини, пошкоджені клітини власного організму	Нав'язані маніпулятивні контраргументи , що призводять до маніпулятивних зрушень у переконаннях і думках людей
Імунітет – здатність до опору чужорідним агентам	Здатність живого організму чинити опір інфекції	Здатність людей зберігати свої переконання та ставлення в умовах маніпулятивних впливів
Імунна система – сукупність елементів організму, які захищають його від чужорідних агентів. Функції: розпізнавання загрози, вироблення відповіді (протидії), нейтралізація загрози, запам'ятовування загрози та відповіді	Складається із сукупності органів, тканин, клітин. Ключові функції виконують лімфоцити: – Т-клітини – розпізнання "свій – чужий"; – В-клітини – вироблення антитіл;– фагоцити, NK-клітини – захоплення та знищення бактерій та вірусів	Складається із сукупності когнітивних процесів. Ключові функції виконують аргументи та контраргументи: (i) адресат піддається контраргументам, які "вибивають" його із зони комфорту; (ii) запускається процес пошуку аргументів для підтвердження своїх переконань та спростування контраргументів

Продовження Таблиці 6

1	2	3
Відповідь імунної системи	Антитіла – білкові сполуки, що виробляються організмом для нейтралізації чужорідних агентів	Аргументи – обґрунтування (доводи, інформація) для підтвердження своїх переконань
Імунна пам'ять – прискорена та посилена специфічна відповідь на повторну взаємодію з чужорідним агентом. Формується як здатність "запам›ятати": 1) кожного чужорідного агента, 2) свою унікальну відповідь	Принцип роботи: Т- та В-лімфоцити утворюються з первинною імунною відповіддю і продовжують циркулювати з кров'ю як носії клітини пам'яті. При вторинній відповіді ці клітини розмножуються, збільшуючи потрібні лімфоцити	Принцип роботи: Аргументи, знайдені під час первинного зіткнення з контраргументами, зміцнюють власні переконання. Це готує мислення до опору наступним, переконливішим повідомленням
Щеплення (імунізація) – створення штучного імунітету	Введення збудника хвороби в здоровий організм. Щеплення має бути досить сильним, щоб спровокувати вироблення антитіл, але не настільки, щоб викликати важку інфекцію	"Вприскування" контраргументів в інформаційне поле. Контраргументи мають бути досить сильними, щоб породити бажання вступити в полеміку, але не настільки сильними, щоб змінити власну думку людини
Вакцина	Штучно створений препарат, що складається з ослаблених збудників хвороб	Штучно розроблені слабкі контраргументи, які легко спростувати

Його спростування ("prebunk") дозволить надати психологічний опір майбутнім переконливим інформаційним атакам.

Багатообіцяючим засобом для щеплення виявились ігри через їх потенційну розважальну цінність та обсяг добровільного сприйняття, а також рівень когнітивних зусиль, необхідних для їх виконання (*Roozenbeek & Van der Linden, 2021*).

Можна рекомендувати використання з метою щеплення проти дезінформації онлайн ігри на основі вибору, в яких **студенти беруть на себе роль зловмисника**:

– браузерна онлайн-гра **Bad News / погані новини** (www.getbadnews.com) для боротьби з дезінформацією, створена DROG та Кембриджським університетом, у якій гравці беруть на себе роль виробника фейкових новин;

– українська версія гри-щеплення для протидії фейковим новинам – онлайн-гра "**Маніпулятор**" (https://texty.org.ua/d/manipulator-game/) створена незалежним виданням TEXTY.ORG.UA у співпраці з Інститутом масової інформації (ІМІ), де так само гравці беруть на себе роль виробника фейкових новин, але вже в українському контексті;

– он-лайн гра **Harmony Square / Площа Гармонії** (www.harmonysquare.game), розроблена DROG, Глобальним центром взаємодії Державного департаменту США та Кембриджським університетом) бореться не лише з дезінформацією, але й з поляризацією суспільства; гравці беруть на себе роль "Головного спеціаліста з дезінформації" для зловмисної організації, їм доручено організувати кампанію впливу, щоб роз'єднати людей на площі Гармонії;

– онлайн-гра **Go Viral! / Ставай вірусним!** (www.goviralgame.com), розроблена DROG, Кембриджським університетом та Кабінетом Міністрів Великобританії) зосереджується на дезінформації про COVID-19;

– онлайн-гра **Cranky Uncle / Вередливий дядько** (www.crankyuncle.com), розроблена Джоном Куком з Університету Monash у співпраці з креативним агентством Autonomy) зосереджена на кліматичній дезінформації. Цікаво те, що Cranky Uncle розроблено для використання у навчальному процесі, а на веб-сайті є посібник для викладача, який пояснює застосування гри як навчального інструменту;

– онлайн-гра **ДемоГратія** (https://www.demogratia.platfor.ma), яка розроблена на основі курсу з громадянської освіти "Демократія: від теорії до практики", створеного Міжнародною фундацією виборчих систем (IFES) в Україні для закладів вищої освіти. Тут пропонується набір життєвих ситуацій, які вимагають застосування на практиці методів громадянської участі. Гра пропонує гравцю спробувати себе у різних ролях та в таких ситуаціях, де (як і в реальності) не існує правильних відповідей.

Також можна зробити важливі методичні висновки з практики застосування теорії інокуляції у навчальному процесі:

– надаючи приклади ворожих наративів, потрібно пам'ятати, що це – патогени або контраргументи (табл.8), які обов›язково мають бути спростовані. Не слід сподіватись, що студенти впораються самостійно. Більш того, потрібна ретельна підготовка до спростування (до процедури "prebunk") та пошуку відповідних джерел та алгоритмів. Якщо така робота не підготовлена – краще утриматись від подібних прикладів, бо вони можуть перетворитись з "щеплення" на "хворобу", тобто привести до переконань, вигідних маніпулятору;

– поступовий перехід від легкого матеріалу до складного – дуже важливий. Це означає, що трудомістка робота з пошуку аргументації та створення багатошарових висновків, яка застосовується без попередньої підготовки студентів, може мати зворотній ефект. Складні конструкції критичного мислення виглядають менш привабливо ніж прості та зрозумілі "наративи-фастфуди", створені маніпуляторами. Важливо розпочати з простих аргументів та завдань, поступово переходячи до більш складних та неоднозначних моделей.

Більш глибоке застосування теорії щеплення пропонується як фундамент нової техніки навчання – інтелектуальний спаринг.

8.2. Методика інтелектуального спарингу

Системи штучного інтелекту і люди приймають рішення по-різному, проте вони вразливі до гібридних загроз (*Terziyan et al., 2018*). Одним з підходів до створення механізмів захисту від спроб нападника зірвати процес прийняття рішень є зіграти на схожостях

реакцій штучних та природних систем на гібридні атаки. Ідея полягає в тому, щоб провести паралелі між біологічними процесами, що відбуваються у голові людини, яка обирає одну з можливих альтернатив у точці прийняття рішень, і машинною логікою вибору вірного рішення (*Kaikova et al., 2022*).

Певні механізми, відпрацьовані у природі, довели свою ефективність, а значить, є ймовірність успіху у випадку запозичення їх для нових завдань у цифровому світі.

Розуміння цього підштовхує вчених до пошуку відповідей на безпекові запитання паралельно у когнітивних, суспільних та комп'ютерних науках, а також запозичення успішних результатів однієї галузі в інших. Так, фахівці із кіберзахисту копіюють біологічні процеси і механізми, розробляючи системи штучного інтелекту.

Для того, щоб створити свого роду "когнітивний імунітет" у людей, які приймають рішення, копіюється загальний механізм цифрового імунітету (зокрема, і цифрову вакцинацію), що використовується для систем штучного інтелекту із машинним навчанням (AI/ML) (*Branytskyi et al., 2022*). Вакцинація відбувається за допомогою змагального тренування. Її ефективність підтверджується теорією інокуляції, яка пояснює, як ставлення до складних проблем та людські переконання можна зробити більш стійкими до різноманітних викликів.

Теорія когнітивної інокуляції заснована за аналогію, розглянутою вище біологічною імунізацією та соціальним щепленням. Вона полягає у тому, що процес введення ослабленої дози вірусу для активації вироблення антитіл (щоб допомогти надати стійкість організму до майбутньої інфекції) можна аналогічним чином застосувати до контексту обробки інформації. Іншими словами, шляхом попередження людей та атакування їх суттєво послабленими дозами поведінкових викликів, стає можливим підняти рівень когнітивного опору або згенерувати "ментальні антитіла" проти майбутніх спроб переконання, частково через зміцнення структури мереж асоціативної пам›яті (*Compton, 2005*).

Предмет тренування треба шукати у когнітивно вразливих областях простору прийняття рішень: важливо обирати такі питання (професійні, соціальні, політичні тощо), де суспільство ще не має

єдиної (спільної) думки, а можливі варіанти рішень розбивають спільноту майже навпіл (50/50).

Приклад набору проблем-дилем, що використовується як стимул для змагальної підготовки (станом на 2021 рік), представлений в *Kaikova et al., 2022*. Зокрема такі набори дилем можна використовувати для вимірювання когнітивного статусу людини та його динаміки до, під час та після змагальної підготовки.

Кожен, кому пропонуються ці питання, повинен виконати когнітивну самооцінку, тобто оцінити особисту важливість кожного питання (у відсотках) та надати власну відповідь (рішення) на кожне питання, зазначаючи ступінь власної впевненості (відсоток для рішення "ТАК" проти відсотка для рішення "НІ"). Оптимальний набір питань для змагальної підготовки складається з дилем, які ділять студентів на рівні підмножини за відповідями.

Інтелектуальний спаринг – це змагальне тренування у вигляді інтелектуального бою у класі, який проводиться у формі диспуту між трьома групами студентів разом з викладачами (команда "Атакуючі", команда "Захисник" і команда "Арбітр", як показано на рис. 4, взаємозв'язок між якими копіює ідею архітектури змагальних нейронних мереж (GAN або Generative Adversarial Networks) (*Terziyan et al., 2021*).

Відомо, що диспут часто зміцнює учасників у їхніх власних думках і цінностях, тому тренування, подібне до диспутів, використовується для підвищення стійкості (resilience and robustness) цінностей та мислення учасників.

Команда «Нападник» винаходить запит "Дилема" для Захисника. Дилема вимагає відповіді (вибір із двох варіантів) і має багатоаспектну природу, що розділяє спільноту майже навпіл. Мета нападника насправді не неправильний вибір, а скоріше плутанина та максимальна (близько п'ятдесят на п'ятдесят) розбіжність всередині команди Defender. Тобто, чим більше розбіжностей, тим кращі результати нападника.

Команда «Захисник» повинна відповісти на "Дилему" вибором однієї спільної відповіді (керівник групи робить вибір з урахуванням аргументованого індивідуального вибору членів команди), зазначивши ступінь впевненості (залежно від результату

голосування). Перед цим кожен член команди (кожен відповідає за певний аспект проблеми) ділиться аргументами на користі власного вибору із командою. Мета захисника – зробити правильний вибір (з точки зору Арбітра) з високою впевненістю; тобто чим більше впевненості у правильності вибору, тим краще виступає Захисник.

Команда «Арбітр» має найвідповідальнішу роль надання зворотного зв'язку, іншими словами, реагування по кожній ітерації процесу на дії двох інших команд (нападників та захисників), підкріплюючи реакцію конкретними аргументами. Зворотній зв›язок містить числову оцінку якості запиту зловмисника та якості відповіді від Захисника з детальними коментарями. Очікується, що відгук у такому форматі допоможе покращити продуктивність обох команд-конкурентів на наступних ітераціях процесу. Тобто арбітр фактично є фасилітатором навчального процесу.

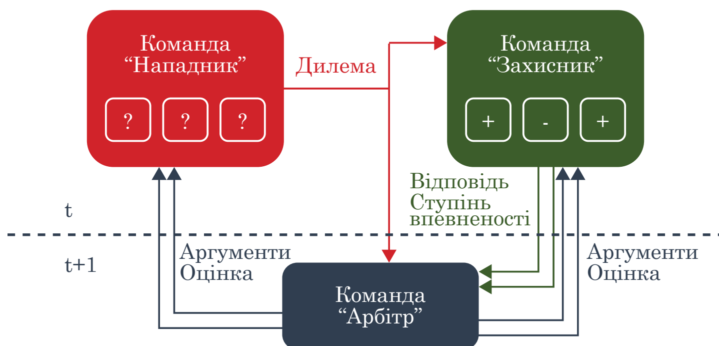


Рис. 3. Схема інтелектуального тренінгу, що моделює процеси в архітектурі Generative Adversarial Networks: одночасне навчання трьох команд студентів "Нападник", "Захисник" та "Арбітр" під час диспутів (*Kaikova et al., 2022*)

Передбачається, що під час тренувального процесу кожен студент хоча б один раз зіграє у кожній із трьох команд ("Атакуючий", "Захисник" і "Арбітр").

Ідеальний інструктор (викладач) такого спарингу має бути не стільки "двигуном" чи "провідником" змагального процесу навчання (або когнітивної вакцинації), скільки "каталізатором" цього процесу. При цьому бажано мати такі три якості:

– пристрасть (включаючи ентузіазм і натхнення);
– імпровізація (включаючи винахідливість і творчість;
– толерантність (у тому числі скромність і самокритичність).

Такі тренінги спрямовані на потребу суспільства, наприклад, українського, знайти "академічну вакцину" (WARN-вакцину) для підняття свідомості громадян та їхнього імунітету проти гібридних загроз, зокрема, когнітивного хакерства.

Зміст курсів WARN по суті слугує профілактичною вакциною, здатною зміцнити імунітет студентів від гібридних атак (як внутрішніх, так і зовнішніх) на їхню свідомість, совість, відповідальність, культуру та систему цінностей. Найважливішим академічним нововведенням є наступне:

Мета інтелектуального спарингу – це не оновлення особистих знань, навичок, переконань чи цінностей, а формування навичок для забезпечення надійності та стійкості переконань чи цінностей при створенні умов для їх розвитку

Тому новий підхід до інтелектуального спарингу (змагальної підготовки WARN) так само відрізняється від зомбування студентів новим змістом, наскільки процес вакцинації відрізняється від процесу отруєння. Студентами таких курсів є різні майбутні, знання та навички яких мають бути не тільки повними, але й надійними, щоб служити важливим фактором для сталого суспільства зі стійкими політичними, бізнесовими та виробничими процесами.

Джерела посилань

Branytskyi, V., Golovianko, M., Gryshko, S., Malyk, D., Terziyan, V., Tuunanen, T. (2022). Digital clones and digital immunity:

adversarial training handles both. International Journal of Simulation and Process Modelling, 18 (2), 124–139. doi: https://doi.org/10.1504/ijspm.2022.126106

Compton, J.; Dillard, J. P., Shen, L. (Eds.) (2013). Inoculation theory. The SAGE handbook of persuasion: Developments in theory and practice. Sage Publications, Inc., 220–236. doi: https://doi.org/10.4135/9781452218410.n14

Compton, J. A., Pfau, M. (2005). Inoculation Theory of Resistance to Influence at Maturity: Recent Progress In Theory Development and Application and Suggestions for Future Research. Annals of the International Communication Association, 29 (1), 97–146. doi: https://doi.org/10.1080/23808985.2005.11679045

Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., Titova, L. (2022). Hybrid Threats against Industry 4.0: Adversarial Training of Resilience. E3S Web of Conferences, 353, 03004. doi: https://doi.org/10.1051/e3sconf/202235303004

Roozenbeek, J., Van der Linden, S. (2021). Inoculation Theory and Misinformation. Riga: NATO Strategic Communications Centre of Excellence, 21. Available at: https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217

Terziyan, V., Golovianko, M., Gryshko, S.; Dimitrov, K. (Ed.) (2018). Industry 4.0 intelligence under attack: From cognitive hack to data poisoning. Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures. IOS Press, 110–125. doi: https://doi.org/10.3233/978-1-61499-888-4-110

Terziyan, V., Gryshko, S., Golovianko, M. (2021). Taxonomy of generative adversarial networks for digital immunity of Industry 4.0 systems. Procedia Computer Science, 180, 676–685. doi: https://doi.org/10.1016/j.procs.2021.01.290

ДОДАТОК А. ГЛОСАРІЙ ВАРГЕЙМІНГУ

Глосарій складено за матеріалами:

Cancian, M., Cancian, M., Heginbotham E. (2023). The First Battle of the Next War. Wargaming a Chinese Invasion of Taiwan. A Report of the CSIS International Security Program. CSIS, 165. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/230109_Cancian_FirstBattle_NextWar.pdf

The Development, Concepts and Doctrine Centre (2017). Wargaming Handbook. DCDC. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

№	Англійська термінологія	Українська термінологія
1	**Adjudication** is the act of determining the outcome of player decisions	**Винесення судового рішення** це акт визначення результату рішень гравців
2	**After action review** A facilitated discussion that actively involves the training audience	**Огляд після дії** Спрощена дискусія, яка активно залучає навчальну аудиторію
3	**Base case** The most likely assumption about each individual variable	**Основний варіант** Найбільш ймовірне припущення щодо кожної окремої змінної
4	**Base scenario** The scenario in which all assumptions are set to the base case	**Базовий сценарій** Сценарій, у якому всі припущення налаштовані на базові значення

№	Англійська термінологія	Українська термінологія
5	**Black** Colour used to represent organized and transnational organized criminals	**Чорний** Колір, який використовується для представлення транснаціональних організованих злочинців
6	**Blue** Colour used to represent friendly or allied forces	**Блакитний** Колір, який використовується для представлення дружніх або союзних сил
7	**Brown** Colour used to represent neutral actors or civilian population	**Коричневий** Колір, який використовується для представлення нейтральних акторів або цивільного населення
8	**Campaign analysis** A method involving the use of a model and techniques for managing uncertainty to answer questions about military operations	**Аналіз кампаній** Метод, що передбачає використання моделі та методів управління невизначеністю для отримання відповідей про військові операції
9	**Constructive simulation** Simulated people using simulated systems	**Конструктивне моделювання** Моделювання людської поведінки за допомогою симуляторів
10	**Descriptive data** Data on the occurrences of a given iteration, for example, who won and how many missiles were fired	**Описові дані** Дані про явища певної ітерації, наприклад, хто виграв і скільки ракет було випущено
11	**Event** An inserted major occurrence or a sequence of related incidents which fit into an exercise framework and are supported by incidents and injections designed to generate response(s) from the exercise participants	**Подія** Головне явище чи послідовність пов’язаних інцидентів, які вписуються у структуру навчань і підтримуються інцидентами, призначеними для генерування відповіді(й) від учасників навчань

№	Англійська термінологія	Українська термінологія
12	**Excursion case** Any alternate assumption wherein one or more of the variables is set to be different than the base case	**Нестандартний варіант** Будь-яке альтернативне припущення, в якому одна або більше змінних встановлені як відмінне від базового значення
13	**Excursion scenario** Any scenario wherein one or more variables are set to an excursion case	**Нестандартний сценарій** Будь-який сценарій, у якому для однієї або кількох змінних встановлено нестандартне значення
14	**Incident** An element or subset of an event. It is an action or situation that provides greater clarity to an event by using injections to bring an incident to the attention of the exercise participants for whom it was created	**Інцидент** Елемент або підмножина події. Це дія або ситуація, яка забезпечує більшу ясність події за допомогою вливань, щоб привернути увагу учасників до події, для яких вона була створена
15	**Iteration** One specific play through of the game under any scenario	**Ітерація** Одне конкретне проходження гри за будь-яким сценарієм
16	**Game** The overall project rather than a particular iteration or play-through	**Гра** Загальний проект, а не окрема ітерація чи проходження
17	**Green** Colour used to represent indigenous security forces	**Зелений** Колір, який використовується для представлення місцевих сил безпеки
18	**Live simulation** Real people using real systems	**Симуляція в реальному часі** Реальні люди, які використовують реальні системи
19	**Model** A mathematical or otherwise logically rigorous representation of a system or a system's behavior	**Модель** Математичне чи інше логічно точне представлення системи або поведінки системи

№	Англійська термінологія	Українська термінологія
20	**Net assessment** The comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations	**Чиста оцінка** Порівняльний аналіз військових, технологічних, політичних, економічних та інших факторів, що визначають відносну військову спроможність націй
21	**Operations research** The analytical study of military problems undertaken to provide a scientific basis for decision on action to improve military operations	**Дослідження операцій** Аналітичне дослідження військових проблем, яке проводиться з метою забезпечення наукової основи для прийняття рішень щодо дій з покращення військових операцій
22	**Setting** A geographic and strategic situation designed to provide all the conditions required to support the achievement of high level exercise aims and objectives. It can be real world, fictionalised or synthetic, is the framework on which the scenario can be developed	**Установки** Географічне та стратегічне положення, призначене для забезпечення всіх умов, необхідних для підтримки високого рівня гри. Це може бути реальний світ, вигаданий або синтетичний, це основа, на якій можна розробити сценарій
23	**Simulation** A method for implementing a model over time	**Симуляція** Метод реалізації моделі в часі
24	**Structured judgment** Any analysis that lays out assumptions in a logical, evidence-based argument that leads to a clear conclusion	**Структуроване судження** аналіз, який викладає припущення в логічну, засновану на доказах аргументацію, що веде до чіткого висновку
25	**Scenario** 1. A set of assumptions about each variable that provides the basis for playing one iteration of the game.	**Сценарій** 1. Набір припущень щодо кожної змінної, який забезпечує основу для однієї ітерації гри.

№	Англійська термінологія	Українська термінологія
	2. The background story that describes the historical, political, military, economic, cultural, humanitarian and legal events and circumstances that have led to the specific current exercise crisis or conflict. The scenario is designed to support exercise and training objectives and, like the setting, can be real, fictionalised or synthetic as is appropriate	2. Передісторія, яка описує історичні, політичні, військові, економічні, культурні, гуманітарні та правові події та обставини, які призвели до конкретної поточної кризи чи конфлікту у навчанні. Сценарій розроблений для підтримки цілей тренувань і тренувань і, як і обстановка, може бути реальним, вигаданим або синтетичним, залежно від обставин
26	**Systems analysis** The process of studying a procedure or business to identify its goal and purposes and create systems and procedures that will efficiently achieve them	**Системний аналіз** Процес вивчення процедури або діяльності, щоб визначити їх мету, задачі та створити системи і процедури, які ефективно їх досягнуть
27	**Unstructured judgment** Any analysis that lacks evidence, logical structure, or transparency	**Неструктуроване судження** Будь-який аналіз, якому бракує доказів, логічної структури чи прозорості
28	**Variable** A condition likely to have an impact on the analysis about which the project team must make an informed assumption	**Змінна** Умова, яка може вплинути на аналіз, щодо якої команда повинна зробити обґрунтоване припущення
29	**Wargaming** A simulation, by whatever means, of military operations involving two or more opposing forces, using rules, data, and procedures designed to depict an actual or assumed real life situation	**Варгеймінг** Симуляція військових дій будь-якими засобами за участю двох чи більше протиборчих сил з використанням правил, даних і процедур, призначених для відтворення фактичної чи припущеної реальної життєвої ситуації

ДОДАТОК Б. ПРИКЛАД ОРГАНІЗАЦІЇ ВАРГЕЙМІНГУ ДЛЯ СПЕЦІАЛЬНОСТІ «ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ»

Михайло Білоконь[1]
[1]Харківський національний університет імені В. Н. Каразіна

Об'єднано декілька методів навчання: **метод кейс-стаді** (розбір конкретних ситуацій); **метод ділової гри** (моделювання конкретних можливих ситуацій, що відносяться до предмету навчання); інтегровано варгеймінг через **змагальні методи** – моделювання гібридного впливу, засноване на сценаріях в яких результат і послідовність подій впливають на рішення, що приймаються гравцями.

1 етап. Ознайомлення здобувачів із методами інформаційного впливу та тактиками поширення фейків (такими як клік-бейти, упереджена подача інформації, вигадані новини, etc.), та із порадами щодо відповідального споживання інформації.

2 етап. Розділення здобувачів на чотири групи (публічні службовці, представники громадянського суспільства, представники ЗМІ та група гібридного впливу "Червоні"). Ознайомлення здобувачів із заздалегідь підготовленими кейсами (описом наближеної до реальності ситуації, та роллю яку кожна група має виконувати).

3 етап. Відбувається моделювання "консультацій із громадськістю". Кожна група діє відповідно до своєї ролі: "Публічні службовці" проводять консультацію, самостійно організуючи процес; "Представники громадянського суспільства" представляють свою позицію щодо питань, визначених у кейсах; "Група впливу", використовуючи методи спотворення інформації, намагається реалізувати або просування потрібного їм наративу, або внести дестабілізацію у процес комунікації громадськості та публічної влади;

"ЗМІ" незалежно висвітлюють процес, роблять нотатки, та намагаються незалежно оцінити роботу інших груп.

Дії кожної групи відбуваються по черзі. Цей процес мають організовувати "публічні службовці".

4 етап. "Публічні службовці" приймають певне обґрунтоване рішення за підсумками 3 етапу. "ЗМІ" готують коментар щодо цього рішення.

5 етап. Рефлексія щодо заняття, під час якої здобувачі опрацьовують здобуті знання, навички, та розуміння інформаційного впливу та гібридних загроз у процесі комунікації громадськості та публічної влади.

Наукова публікація

**Едуард Балашов, Михайло Білоконь,
Тетяна Борозенцева, Марія Головянко, Світлана Гришко,
Тарас Жовтенко, Оксана Карпенко, Ольга Копієвська,
Олександр Котуков, Павло Худ**

МЕТОДИКА НАВЧАННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Посібник

ТОВ "ТЕХНОЛОГІЧНИЙ ЦЕНТР ГРУП"
вул. Шатилова дача, 4, м. Харків, Україна, 61165
Свідоцтво про внесення суб’єкта видавничої справи
No. 7582 від 01.02.2022
Опубліковано 26.10.2023 р.

«Академічна протидія гібридним загрозам»
№ 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP

МЕТОДИКА НАВЧАННЯ
В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Посібник

Харків, 2023

УДК 378.147:351.861
М 54

Автори:
Едуард Балашов, Михайло Білоконь, Тетяна Борозенцева, Марія Головянко, Світлана Гришко, Тарас Жовтенко, Оксана Карпенко, Ольга Копієвська, Олександр Котуков, Павло Худ

М 54 Методика навчання в умовах гібридних загроз: посібник / Е. Балашов, М. Білоконь, Т. Борозенцева, М. Головянко, С. Гришко, Т. Жовтенко та ін. – Харків: ТОВ "ТЕХНОЛОГІЧНИЙ ЦЕНТР ГРУП", 2023. – 84 с.

DOI: 10.62067/978-617-8242-02-2
ISBN 978-617-8242-02-2 (on-line)

Посібник з методики навчання в умовах гібридних загроз створений як один із результатів проєкту WARN "Академічна протидія гібридним загрозам", за фінансової підтримки програми ЄС Еразмус+, №610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP. Мета проєкту полягає у підвищенні рівня національної безпеки шляхом подолання нестачі суспільних безпекових сервісів, яка виникла через появу гібридних загроз. Це – загрози нового типу, вони створюються скоординованими та синхронізованими діями, які свідомо спрямовані на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів. Головною вразливістю гібридних загроз стає демократичний процес прийняття рішень та всі, хто бере в ньому участь. Люди опиняються незахищеними, якщо не вміють розпізнавати гібридні загрози, визначати не локальну, а загальну мету гібридних впливів, а також – об'єднувати зусилля та захищати свій робочий та соціальний простір від гібридних загроз. Для ефективної протидії цьому новому типу загроз проєкт WARN запровадив превентивне навчання та підготовку громадян як агентів захисту. Це стає можливим завдяки додаванню до будь-якої освітньої програми унікальної компетентності, що спрямована на вміння виконувати свої професійні та громадські обов'язки в неочікуваних, непрогнозованих, навіть – в екстремальних ситуаціях, спричинених гібридними загрозами. Специфічна методика навчання є невід'ємною складовою формування такої компетентності, бо саме вона дозволяє напрацьовувати навички комплексного захисту та протидії гібридним загрозам.

УДК 378.147:351.861
ISBN 978-617-8242-02-2 (on-line)

Цей проект був профінансований за підтримки Європейської Комісії.
Ця публікація відображає лише погляди автора, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься в ній.

ЗМІСТ

СПИСОК ТАБЛИЦЬ

СПИСОК РИСУНКІВ

ВСТУП

Тарас Жовтенко[1]
Едуард Балашов[1]
[1]Національний університет "Острозька академія"

Формування безпекової політики України відбувається в умовах активного протистояння сучасним безпековим викликам, новим та унікальним не лише для нашої держави, але й для світу загалом.

На ці виклики нашаровуються динамічні процеси сучасних геополітичних змін у регіоні та світі, які характеризуються закінченням глобальної конфронтації, викликаної ідеологічним протиборством двох світових систем. Разом з тим, сьогодні залишаються протиріччя, що пов'язані з розбіжностями національних інтересів, цілей, позицій України на внутрішньому, регіональному та світовому рівнях.

Викликають занепокоєння такі негативні чинники, як поляризація рівня життя, деградація навколишнього середовища, розповсюдження загрозливих хвороб, виникнення невідомих раніше масових захворювань, неконтрольована міграція, етнічні та конфесійні напруження, збільшення масштабів і частоти техногенних катастроф. Вони призводять до пересування центру традиційних загроз (збройне вторгнення) у бік нетрадиційних, зростання яких значною мірою зумовлено інформаційною відкритістю сучасного суспільства, вразливістю великих індустріальних міст.

Ці процеси лежать в основі тренду "гібридизації" сучасних загроз національній та міжнародній безпеці.

Гібридне протистояння України та російської федерації, яке почалося з військово-політичної та інформаційної агресії Кремля на початку 2014 року, практично від самого свого початку поставило під сумнів майже усі засади сформованої системи міжнародної

безпеки. Відтак, для України та країн Західного світу актуальним є пошук адекватної та ефективної системи реагування на виклики та загрози, які принесли з собою ці події.

Відмітною рисою гібридного інструментарію є використання широкого спектру інструментів – від воєнної сили (регулярних сил та нерегулярних збройних формувань) до активного інформаційно-психологічного впливу в ключових сферах інформаційної інфраструктури противника (дезінформація, пропаганда в традиційних медіа та соціальних мережах, кібератаки, активні заходи спецслужб тощо), використання інструментів політичного, економічного, гуманітарного впливу.

Гібридна агресія характеризується мультидоменністю, одночасним використанням різноманітних комбінацій інструментарію, які варіюються залежно від динаміки гібридного конфлікту, реакції противника та змін безпекового середовища на регіональному та глобальному рівнях.

Для протидії такій комплексній і динамічній загрозі вкрай необхідні нові підходи до розуміння та формування архітектури не лише систем національної безпеки окремих держав. Необхідною умовою ефективної протидії гібридному інструментарію є створення динамічного, комплексного середовища забезпечення безпеки, побудованого у відповідності до логіки самої гібридної загрози – на спільних засадах універсальності та мультидоменності.

Формування такого середовища – не лише сфера відповідальності національних урядів окремих держав та їх секторів безпеки та оборони. Для ефективної протидії гібридним інструментам та створення надійної системи захисту необхідно залучати усі домени-потенційні об’єкти гібридних атак, а також створити надійну систему синергії між академічною і практичною сферами суспільства і держави.

Запорукою цього є формування універсальної і сучасної системи науково-практичного розуміння природи та сутності гібридної загрози та її складових.

Існування такої системи неможливе без розробки новітньої методики для широкого кола академічної спільноти та фахівців-практиків з вивчення, виявлення, аналізу та протидії сучасним гібридним загрозам.

Така інноваційна методика "гібридного навчання" має базуватися на основі:

– проактивного захисту: фокусується на виявленні потенційних загроз;

– змагальних моделей навчання (на основі сучасного штучного інтелекту);

– предметно-орієнтованих ігор;

– інтелектуальної технології моделювання сценаріїв гібридних загроз, специфічних для реалій України.

Пропонований посібник фокусується на плануванні та проведенні лекційних та практичних занять відповідно до нових методик, проведення тематичних воркшопів, майстер-класів, використанні технологій бренйшторму та симуляцій, змагальних ігор та інтелектуальних спарингів.

Подяка

Ми вдячні експертам з Університету м. Ювяскюля (Фінляндія) – проф. О. Кайковій та проф. В. Терзіяну за неординарні ідеї, унікальну співпрацю, організаційні та дослідницькі можливості, надані нашій команді, – всього того, що спрямовувало та надихало при створенні цього посібника.

Також ми вдячні експертам дослідницької організації TNO (Нідерланди), завдяки яким ми не лише познайомились із світом навчальних ігор, але й отримали можливість занурились в їх дивовижну атмосферу.

1. ОСВІТА ЯК ЗАХИСТ ВІД ГІБРИДНИХ ЗАГРОЗ

Світлана Гришко[1]
Марія Головянко[1]
[1]Харківський національний університет радіоелектроніки

1.1. Розуміємо небезпеку: на що потрібно звернути увагу

Навчання завжди відігравало важливу роль для розвитку людства та підтримки його життєздатності:

– навчання дає людям знання та навички, які потрібні для праці та життя;

– навчання допомагає розвивати мислення та креативність, виховує здатність аналізувати інформацію, ставити питання, шукати відповіді, розв›язувати проблеми;

– навчання допомагає людям розуміти інших людей та розвивати толерантність та розуміння різних культур та світоглядів.

Ці фундаментальні задачі освітнього процесу зберігають свою актуальність і сьогодні. Але змінюються умови їх реалізації: по-перше, змінюються умови самого процесу навчання; по-друге, змінюються умови життя, до яких викладачі готують своїх учнів. Серед таких змін – поява гібридних загроз. Особливістю ситуації є те, що професійний безпековий сектор не має достатніх можливостей та ресурсів для самостійної протидії складним гібридним загрозам. Він потребує можливості спиратись на обізнаність суспільства про гібридні загрози та способи захисту в таких умовах. Це визнається низкою офіційних документів, наприклад:

– спільна рамка ЕС та НАТО з протидії гібридним загрозам вказує, що підвищення обізнаності громадськості про гібридні загрози

є одним основних факторів розвитку соціальної стійкості (*European Council, European Commission, NATO, 2016; п. 3.2*);

– в огляді НАТО відзначається: для протидії гібридним загрозам "важливість освіченої громадськості не можливо перебільшити" (*Hagelstam, 2018*);

– План дій цифрової освіти ЄС розглядає освіту як один з інструментів стійкості суспільства та протидії сучасним викликам (*European Council, European Commission, European Economic and Social Committee, 2020*);

– в огляді НАТО, який охоплює заходи з протидії гібридним загрозам (*NATO, 2023*), підкреслюється важлива роль тренувань, навчання, освіти та співпраці військових та невійськових учасників;

– фінська концепція комплексної безпеки, яка вважається однією з найефективніших в умовах гібридних загроз, базується на підготовленості всього суспільства до несподіваних викликів, включно із стійкістю домогосподарств (концепція "72 години") та обізнаністю суспільства, зокрема – завдяки національним курсам оборони (*Turvallisuuskomitea, 2017*).

Таким чином, навчання, освіта та загальна обізнаність суспільства відіграють одну з ключових ролей для протидії гібридним загрозам. Вони мають закрити нестачу навичок у людей, які приймають рішення щодо розпізнавання гібридних загроз, визначення їх мети, прогнозування наслідків власних дій при гібридних впливах та захисту свого робочого і соціального простору від гібридних загроз.

В рамках роботи над проєктом Еразмус+ "Академічна протидія гібридним загрозам" (**WARN**) 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP була сформульована ключова компетентність, необхідна для забезпечення безпеки суспільства в умовах гібридних загроз (*WARN, 2022*):

> **Компетентність**: здатність адаптувати робочі процеси та особистий простір до складних та непередбачуваних ситуацій, спричинених гібридними загрозами, з урахуванням аспектів соціальної відповідальності.
>
> WARN©

Для того, щоб освітній процес формував таку компетентність, мають бути створені наступні результати навчання:

> **Перший результат навчання:** розуміти комплексну природу, складність, логіку і закономірності гібридних загроз;
> **Другий результат навчання:** виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.
>
> WARN©

Такі результати навчання неможливо забезпечити лише за рахунок оновлення контенту та інформування про новий тип загроз. Потрібно нарощувати й поведінкові навички – адекватну реакцію на "невідомі невідомі", вміння орієнтуватись у несподіваних ситуаціях, швидко та ефективно надавати відповідь у невизначених складних умовах тощо. Для цього, разом із контентом, мають бути оновлені й практики викладання.

Враховуючи, що гібридні загрози мультидоменні, неочікувані, непрогнозовані, знаходяться нижче порогу ідентифікації та не атрибутований, можна визначити наступні задачі нової методики навчання в умовах гібридних загроз:

1. Підвищення освіченості у різних професійних доменах: оскільки гібридні загрози мультидоменні, то прийняття рішень вимагає системного підходу та розуміння того, як працює вся сукупність доменів; особи, які приймають рішення, мають оцінювати всі окремі загрози та ризики як елементи єдиної "картини", а не аналізувати їх окремо.

2. Розвиток критичного мислення: вміння розрізняти джерела та призначення інформації, обмірковувати, аналізувати та ставити питання, дозволяє уникнути впливу маніпуляцій та окремих агентів, що поширюють неправдиву інформацію.

3. Забезпечення когнітивної стійкості: оскільки гібридні загрози націлені на механізм прийняття рішень, то людська свідомість стає полем бою. Мета когнітивної війни полягає у зміненні

не лише того, що думає людина, а й того, як вона думає і діє (*Хопкінс, 2021*). Когнітивна війна прагне посіяти сумніви, запровадити суперечливі наративи, поляризувати громадську думку, радикалізувати групи і спонукати їх до дій, які можуть зруйнувати або розділити згуртоване суспільство. Нова методика навчання має забезпечити когнітивну стійкість, яка надає людині відчуття та розуміння цінностей та змісту без втрати адаптивності та здібності до розвитку.

4. Нарощування навичок співпраці між різними групами населення, між громадськістю та владою: це передбачає вміння налагоджувати механізми співпраці для спільної роботи над виявленням та протидією гібридним загрозам.

5. Забезпечення інформаційної стійкості, яке формує вміння перевіряти та знаходити достовірну надійну актуальну інформацію.

Вказані навички є у фокусі й звичайних освітніх практик, які розвиваються разом із розвитком людського суспільства. Вони важливі для надання необхідних знань та вмінь, розвитку мислення та налагодження взаємодії та співпраці. Тож, вони мають використовуватись й для навчання в умовах гібридних загроз. Нова методика має на меті спрямувати вибір викладачів у тих педагогічних напрацюваннях, які є особливо корисними для навчання в умовах гібридних загроз, а також на додаток – запропонувати й специфічний методичний підхід до навчання, який містить поєднання змагальних практик в області штучного інтелекту, проактивних педагогічних підходів та спортивного тренування – **інтелектуальний спаринг**.

Гібридні впливи чинять тиск й на сам освітній процес, тому для ефективного навчання в умовах гібридних загроз потрібно врахувати наступні особливості:

1. Використання онлайн-технологій та цифровий твінінг (дублювання): умови гібридних загроз можуть призвести до того, що фізичні зустрічі між викладачами та студентами стають складнішими. Використання онлайн-технологій, таких як відеоконференції та платформи для дистанційного навчання, віртуальні лабораторії тощо, може допомогти зберегти зв›язок між викладачами та студентами та забезпечити продовження процесу навчання.

2. Фокус на здоров›ї та добробуті: умови гібридних загроз можуть призвести до підвищення рівня тривоги та стресу серед студентів та викладачів. Для забезпечення ефективного навчання в таких умовах потрібно подбати не лише про методи донесення чутливого контенту, але й сформувати певну стійкість – підготувати студентів до роботи з таким контентом.

3. Гнучкість та адаптивність: умови гібридних загроз можуть бути дуже непередбачуваними, тому важливо бути гнучким та адаптивним. Це означає, що викладачі та студенти можуть потребувати змінювати свій підхід до навчання та залежно від ситуації швидко реагувати на зміни.

1.2. Окреслюємо межі: термінологія та критерії важливі, як ніколи

Гібридні впливи розмивають системи цінностей, граючи на межі понять. Якщо стерти чітку грань між категоріями (війна-мир, добре-погано, друг-ворог тощо), то виникає "сіра зона" невизначеності, в якій прийняття рішень буде нестійким, потенційно вразливим. Тому викладання дисциплін з тематикою гібридних загроз вимагає уважної роботи з термінологією та критеріями прийняття рішень.

Кейс: визначення поняття «гібридні загрози».

Існує велика кількість визначень "гібридних загроз". Для науки, яка формується, це не є чимось незвичайним. Але у новому безпековому ландшафті навіть розуміння гібридних загроз стає полем бою. Як правило, всі існуючі визначення акцентують увагу на наступних ознаках гібридних загроз:

– мультидоменність, як інструментів, так і вразливостей;

– асиметричність;

– перебування нижче порогу атрибуції, тобто неможливість ідентифікувати діяльність як злочинну і однозначно визначити, хто несе за неї відповідальність.

Це дійсно важливі ознаки. Чи достатньо цього? Скоріш за все, викладач, який обмежиться лише такими ознаками, стикнеться з наступними відповідями:

Студент № 1: "Гібридні загрози відомі з глибокої давнини, в них немає нічого нового, просто технології були іншими: наприклад, отруєння колодязів або підкуп оборонців з тим, щоб вони відкрили ворота фортеці тощо".

Студент № 2: "США проводить гібридну війну проти Ірану та країн Південної Америки".

Студент № 3: "Війна НАТО за Україну – це лише один із етапів гібридної війни, яку Захід розв'язав проти Росії".

Такі відповіді означають, що відбулась підміна поняття: студенти сприйняли асиметричні впливи або комбінацію інструментів як вичерпні ознаки гібридних загроз. Якщо саме такі "знання" студент винесе з освітнього процесу, то він стає **легкою здобиччю маніпуляторів**. Знаючи лише те, що в світі відбуваються асиметричні впливи та приховані операції, такий студент стане ще більш вразливим для теорій змови, перекручення, підміни понять та інформаційно-психологічних операцій гібридних зловмисників.

Неправильне розуміння основних понять гібридних загроз призводить до того, що стійкість студентів буде підірвана навіть більше, ніж якби вони взагалі не проходили навчання.

Рекомендація: при створенні контенту курсів слід спиратись на системні авторитетні дослідження на кшталт тих, що оприлюднює Європейський центр передового досвіду з протидії гібридним загрозам Hybrid CoE, та ретельно опрацьовувати їх зі студентами.

У визначенні Hybrid CoE, "гібридні загрози – це скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів, за використанням широкого кола засобів". Тобто, серед ключових характеристик – націленість таких загроз на вразливості демократії. А чи мають студенти ясне розуміння того, які є особливості та різновиди демократичного способу прийняття рішень? Які демократичні механізми та інституції існують? Що являють собою демократичні цінності? Що є силою демократії та які вона має слабкі місця? Як показала практика, корисним є розгляд конкретних прикладів про те, як реагують на загрози авторитарні та демократичні країни, як-от, наприклад, обговорення COVID-кейсу у контексті проблеми "безпека vs демократичні цінності" (авторитарні та демократичні країни

використовували різні підходи для боротьби з наслідками ковід-пандемії). Часто студенти самі роблять висновки про те, що демократія, надаючи важливі переваги для вільного розвитку суспільства, містить й специфічні вразливості.

Приклади міркувань студентів, які пройшли подібні обговорення та з якими були чітко окреслені особливості демократичних механізмів прийняття рішень:

Студент № 1: "Гібридні загрози – це спроба "хакнути" сучасну демократію, знайти слабину у механізмах прийняття рішень громадою та вдарити саме в її сутність".

Студент № 2: "Не має можливості спрямувати гібридні загрози проти авторитарних країн, бо в них нема таких "органів", які б могли бути вражені цими загрозами".

Студент № 3: "Демократичні країни не можуть відплатити гібридним зловмисникам тією ж монетою, бо, по-перше, у демократіях існують механізми-запобіжники до маніпуляцій, а по-друге, у авторитарних країнах думка громадян не відіграє ролі у прийнятті рішень".

Студент № 4: "Гібридні загрози ставлять демократію перед дилемою безпеки – або потрапити під удари, або згорнути демократію. В таких ситуаціях авторитарним країнам простіше, бо в них лише одне завдання – вийти з-під удару".

Якщо приділити час на обговорення таких суттєвих ознак, це дозволить зняти багато непорозумінь у подальшій роботі. Це дозволить провести чітке розмежування між політичними, інформаційними та військовими операціями (до яких вдається кожна держава) та гібридними впливами (до яких вдаються авторитарні країни-ревізіоністи). А головне – це сформує міцний фундамент для громадської стійкості студентів через обізнаність про справжні загрози.

Висновок: дисципліни з протидії гібридним загрозам вимагають від викладача особливо уважного підходу до термінологічного апарату. Перш ніж переходити до практичних занять та вправ, викладач має впевнитись, що він спілкується зі студентами однією мовою. Для того, щоб зорієнтуватись в термінології, викладачам може стати в нагоді Глосарій, створений в рамках WARN-проєкту (*Гришко та ін., 2021*).

1.3. Підтримуємо етичні системи цінностей

Прийняття рішень базується на певних системах цінностей, які виконують роль внутрішнього арбітра. Система цінностей містить набір параметрів та критеріїв (правил), за якими відбувається прийняття рішень. Проблема виявляється у тому, що системи цінностей розвиваються разом з особистістю, тобто вони не є константами. Можливість оновлення критеріїв вибору відкриває вразливі моменти для маніпуляцій зловмисників.

Це стає серйозною проблемою й для викладача: з одного боку, – заохочувати гнучкість пріоритетів, що створює умови для розвитку особистості; а з іншого – навчити зберігати стійкість системи цінностей та не піддаватись маніпуляціям.

Вирішення цієї проблеми дозволить сформувати головну компетентність, потрібну в умовах гібридних впливів: вміння зберігати не лише сьогоднішню сталу систему цінностей, але й зберігати здатність для її свідомого неманіпулятивного вдосконалення. Все це обумовлює важливість двох моментів, які мають бути враховані у навчальному процесі:

1. Формулювання та обговорення на заняттях етичних принципів та норм в різних сферах професійної діяльності та громадського життя.

2. Розгляд складних прикладів, в яких немає простих рішень, що дозволить підготувати студентів до стійкості в умовах гібридних загроз.

Часто викладачі дисциплін професійного спрямування на своїх заняттях "не встигають" розглянути приклади з етичними викликами, бо крім обмеженого часу аудиторної роботи, ці приклади занадто складні, можуть завести бесіду в неочікуване русло, мають чутливий контент тощо. Це дійсно складні заняття.

До цього додається ще один виклик – такі заняття вимагають нарощування власної стійкості самого викладача. Це – додаткове ретельне опрацювання великої кількості різних аргументів та можливих напрямків розвитку заняття, розуміння етичних принципів прийняття рішень у складних ситуаціях, психологічна рівновага та делікатність.

Але такі складові на заняттях дуже потрібні. Це не обов'язково мають бути окремі модулі чи спеціальні завдання. Акцент на системі цінностей та етично-складних професійних ситуаціях можна додати до будь-якого заняття. Це необхідний елемент для підготовки студентів до роботи в умовах гібридних загроз.

Гібридні загрози часто називають "**злісними проблемами**" (Wicked problem) через те, що такі проблеми складно або неможливо вирішити внаслідок неповноти, суперечності або мінливості інформації і вхідних умов (Cullen, 2018).

Такі проблеми легко стають мішенню гібридних зловмисників, бо злісні проблеми неможливо вирішити. Прийняття рішень у цій площині не буває легким та вимагає міцної системи цінностей, вміння знайти потрібну інформацію та побачити повну картину, розуміння поняття "справедливість" та моральної готовності обирати краще з поганих рішень.

Рішення злісних проблем завжди міститиме негативні наслідки. Але, на відміну від маніпуляцій, стійкість особи, що приймає рішення, має проявлятись у наступному:

– **пильність:** вміння знаходити та обирати джерела інформації з вимогами до достовірності (підтвердження об'єктивності даних), надійності (підтвердження інформації з кількох джерел), авторитетності (підтвердження експертності джерела) та актуальності (своєчасності);

– **свідомий вибір:** вміння формувати та розмірковувати над аргументами;

– **стійкість:** спроможність приймати ефективні обґрунтовані рішення навіть під впливом негативних чинників.

1.4. Вчимо проактивному захисту

Гібридні впливи досягають своєї мети на рівні окремої людини (особи, яка приймає рішення) через когнітивний злам (cognitive hack). Когнітивний злам містить три складові, які можна назвати "3D":

– дезорієнтація: люди втрачають впевненість у своїх цінностях;

– деморалізація: люди стають абсолютно байдужими своїх цінностей ("пофігізм");

– дестабілізація: люди несвідомо руйнують своє середовище на користь зловмисника через неправильні рішення.

Для того, щоб наш розум створив імунітет проти когнітивного зламу, який є основою гібридних впливів, потрібна "академічна вакцина". Так само, як імунітет людини, захист від гібридних загроз вимагає не лише вміння протидіяти вже відомим загрозам (так званим "відомим невідомим"), але й виявляти та протидіяти "невідомим невідомим" – тобто таким новим типам виплививів, навіть про існування яких ніхто не обізнаний.

Інформація про "Невідомі невідомі" не піддається моніторингу, який побудованій на сприйнятті того, що ми очікуємо сприймати (за допомогою шаблонів розпізнавання або використання набору індикаторів). Це пов’язано з тим, що аналітик ніколи раніше не бачив цієї закономірності і не може мати набір індикаторів для того виду атаки, який раніше ніколи не мав місця або навіть не був уявним. Проблема захисту системи в умовах "невідомих невідомих" атак добре знайома спеціалістам в області кіберзахисту: сукупність технологій, яка використовується в антивірусному програмному забезпеченні для превентивного виявлення потенційно небезпечних вразливостей, створює механізм **проактивного захисту**. Такий принцип стане в нагоді й для захисту осіб, які приймають рішення в умовах гібридних загроз (**рис. 1**).

Проактивна безпека запобігає невідомим раніше атакам. Вона допомагає усувати будь-яку вразливість, яка робить нас сприйнятливими до атак, перш ніж злочинці використають їх.

Рис. 1 дозволяє виявити ключові підходи, які мають бути втілені у навчанні для забезпечення навичок проактивного захисту:

– моделювання поведінки супротивника: потрібно навчити студентів виходити за межи власної позиції і "залазити у шкуру" ворога;

– симуляція атак, протидії, суперництва, спарингів та інших видів конкурентної інтерактивності.

Це означає, що пасивного слухання матеріалу недостатньо для протидії гібридним загрозам. Це вимагає **активного навчання** (Active learning), тобто залученості студентів до емпіричних

завдань. Існує багато форм активного навчання, серед яких корисними для навчання проактивному захисту, є наступні:

1. Експериментальне навчання (experiential learning, ExL) – філософія та методологія, згідно з якою викладачі цілеспрямовано взаємодіють зі студентами у практичному досвіді та зосередженій рефлексії, щоб збільшити знання, розвинути навички та роз'яснити цінності (*Northern Illinois University, 2012a*). Існує велика кількість підходів та методів експериментального навчання, серед яких в умовах гібридних загроз особливу увагу привертають:

– **симуляція** (simulation), яка дозволяє розвивати критичне мислення, самостійне навчання та є ефективним засобом боротьби з неправильними уявленнями студентів (*Caniglia, 2019*). Метод передбачає створення ситуацій, які вимагають швидкої реакції та дії, які стимулюють студентів до проактивної поведінки;

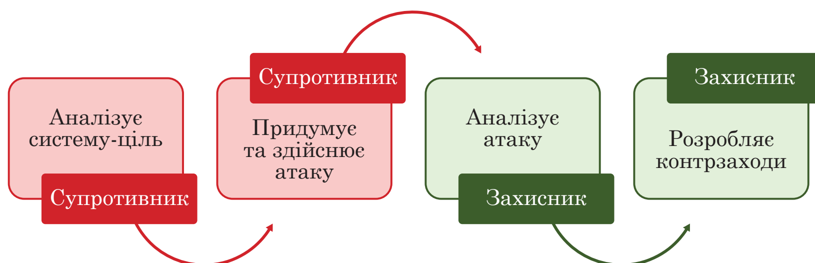
– **рольові ігри** (role-playing): техніка, яка дозволяє студентам досліджувати реалістичні ситуації, керовано взаємодіючи з іншими людьми, щоб отримати досвід і випробувати різні стратегії у певному середовищі (*Glover, 2014*). Цей підхід дозволить студентам побувати зловмисником, але не стати зловмисником. Не можна зрозуміти, як діятиме ворог, якщо не змоделювати його поведінку, не програти можливі сценарії омани, маніпуляції, перекручування, не спробувати атакувати. У такому навчанні важливо зберігати власну систему цінностей. Саме входження у роль та вихід з неї дозволять зрозуміти ворога, але залишитись собою.

2. Діяльне навчання (action learning) – навчання через вирішення конкретної проблеми, який включає виконання дій і рефлексію над результатами (*Corporate Finance Institute, 2022*).

3. Групове або кооперативне навчання (cooperative learning) – метод навчання, що оснований на співробітництві студентів у групах. При такому підході студенти досягають успіхів у навчанні, лише за умови ефективної взаємодії між собою (*SERC Pedagogic Service, n.d.*)

4. Навчання служінню (service-learning) – освітній підхід, який поєднує цілі навчання з громадською роботою (волонтерством), щоб забезпечити прагматичний, прогресивний досвід навчання, одночасно задовольняючи потреби суспільства (*Suffolk University, n.d.*).

5. Ситуаційне навчання (situated learning) – студенти навчаються, беручи активну участь у вирішенні проблем, які формуються у реальних життєвих ситуаціях (*Northern Illinois University, 2012b*).



а) створення реактивного захисту

б) створення проактивного захисту

Рис. 1. Підходи до створення реактивного та проактивного захисту
Складено за Biggio et al., 2014

Ці підходи безсумнівно мають користь для формування у студентів компетентності з протидії гібридним загрозам. Особливості їх застосування та деякі приклади будуть запропоновані до розгляду у наступних розділах.

Джерела посилань

Action Learning (2022). Corporate Finance Institute. Available at: https://corporatefinanceinstitute.com/resources/elearning/action-learning/

Biggio, B., Fumera, G., Roli, F. (2014). Pattern recognition systems under attack: design issues and research challenges. International Journal of Pattern Recognition and Artificial Intelligence, 28 (7), 1460002. doi: https://doi.org/10.1142/s0218001414600027

Caniglia, J. (2019). Simulations as a Teaching Strategy. Kent State University Center for Teaching and Learning. Available at: https://www.kent.edu/ctl/simulation-teaching-strategy

Concept of Comprehensive Security – Building National Resilience in Finland. Turvallisuuskomitea. Available at: https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/

Cooperative learning. Pedagogy in Action, National Science Digital Library. SERC Pedagogic Service. Available at: https://serc.carleton.edu/sp/library/cooperative/index.html

Countering hybrid threats (2023). NATO. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

Cullen, P. (2018). Hybrid CoE Strategic Analysis 8: Hybrid threats as a new 'wicked problem' for early warning. Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

Digital Education Action Plan 2021–2027: Resetting education and training for the digital age (2020). European Council, European Commission, European Economic and Social Committee. Available at: https://education.ec.europa.eu/focus-topics/digital-education/action-plan

Experiential Learning (2012). CITL, Center for Innovative Teaching and Learning. Northern Illinois University. Available at: https://www.niu.edu/citl/resources/guides/instructional-guide/experiential-learning.shtml

Glover, I. (2014). Role-play: An Approach to Teaching and Learning. Technology Enhanced Learning at Sheffield Hallam University.

Available at: https://blogs.shu.ac.uk/shutel/2014/07/04/role-play-an-approach-to-teaching-and-learning/

Gobert, C. (2022). What Is Service-Learning? The Center for Community Engagement, Suffolk University. Available at: https://www.suffolk.edu/student-life/student-involvement/community-public-service/service-learning/what-is-service-learning

Hagelstam, A. (2018). Cooperating to counter hybrid threats. NATO Review. Available at: https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Joint Framework on Countering Hybrid Threats (2016). European Council, European Commission, NATO. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

Situated learning (2012). CITL, Center for Innovative Teaching and Learning. Northern Illinois University. Available at: https://www.niu.edu/citl/resources/guides/instructional-guide/situated-learning.shtml

Updated study programmes. WARN. Available at: https://warn-erasmus.eu/ua/deliverables/updated-study-programmes/

Гришко, С. В., Головянко, М. В., Титаренко, М., Чех, М., Василиця, О., Ланюк, Є. та ін.; Гришко, С. В. (Ред.) (2021). Глосарій з гібридних загроз. Erasmus+ Capacity Building Project WARN, 113.

Хопкінс, Дж. (2021). Протидія когнітивній війні: інформованість і стійкість. НАТО рев'ю. Available at: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html

Co-funded by the
Erasmus+ Programme
of the European Union

ЛЕКЦІЙНЕ ЗАНЯТТЯ

Оксана Карпенко[1]

[1]Державний університет інфраструктури та технологій

Як показала практика, викладання курсів з протидії гібридним загрозам стикається з потужним методичним викликом щодо подачі теоретичного матеріалу:

– з одного боку, проактивний захист (який є головним фокусом такого навчання) вимагає якомога більше практичної підготовки. Зазвичай, така вимога задовольняється через перерозподіл аудиторного навантаження (за рахунок зменшення лекційних занять). Це змушує шукати нестандартні форми подачі теорії, зокрема – й поза аудиторією;

– з іншого боку, студент не зможе навчитись захисту в умовах гібридних загроз лише через практичні вправи, без системного розуміння того, що відбувається у широкому середовищі (а не в локальному осередку). Тобто "бачення без дії – це мрія, а дія без бачення – це жахіття" (східна народна мудрість). Захист від гібридних загроз у першу чергу вимагає комплексної обізнаності осіб, які приймають рішення. Без попереднього опанування теоретичного матеріалу неможливо досягти такого ефекту. Саме тому не можна відкидати жодного педагогічного напрацювання, бо кожний спосіб подачі теоретичного матеріалу може стати у нагоді при викладанні курсів з протидії гібридним загрозам.

Таким чином, серед педагогічних напрацювань потрібно обрати такі рішення, які: (1) дозволяють відповісти на виклик, пов'язаний з подачею теоретичного матеріалу, тобто як помістити великий обсяг мультидисциплінарної теорії у невеликий обсяг часу; (2) надають викладачеві можливість вибору залежно від аудиторії та особливостей курсів; (3) створюють умови для комбінації

існуючих підходів або для адаптивного формування нових підходів до подачі матеріалу.

Технології завжди відігравали важливу роль у навчанні, але вони, як правило, використовувалася лише для підтримки звичайного навчання. Сучасні тенденції надають можливість змінити сам підхід до організації лекційних занять. Це важливо в умовах гібридних загроз, коли навіть знайомство з теоретичним матеріалом вимагає інтерактивного спілкування та проактивності студентів.

Можна виділити такі підходи до організації лекційних занять з використанням новітніх інформаційних технологій (*Bates, 2015; c. 614*):

– **змішане навчання** (blended learning), коли технічні засоби підтримують навчальний процес та не вимагають його перепланування (проведення слайд-лекцій, використання системи управління навчанням для підтримки викладання в аудиторії, для зберігання навчальних матеріалів, тестів та онлайн-обговорень);

– **гібридне або гнучке навчання** (hybrid or flexible learning) – потребує перепланування викладання, щоб студенти могли виконувати більшу частину свого навчання в Інтернеті, приходячи в аудиторію лише для дуже специфічного особистого навчання, наприклад лабораторних або практичних робіт, які неможливо виконати задовільно онлайн;

– **онлайн навчання** (fully online learning) – тобто навчальний процес без навчання в аудиторії, зокрема – курси з отриманням кредитів (дистанційна версія аудиторної освіти); некредитні курси, які пропонуються лише в Інтернеті, наприклад, курси безперервної професійної освіти; повністю відкриті курси, такі як MOOC; та відкриті освітні ресурси, доступні для безкоштовного завантаження в Інтернеті, до яких викладачі або студенти мають доступ для підтримки викладання та навчання.

Гібридне навчання та онлайн навчання передбачають повну перебудову дизайну курсів. При такій організації час на лекційні заняття має бути максимально зменшений (*Bates, 2015; c. 615*). Для того, щоб ефективно донести до аудиторії теоретичний матеріал та використати його у подальшій практичній роботі для протидії гібридним загрозам, слід звернути увагу на наступні підходи:

– "**перегорнуте навчання**" (англ. flipped classroom) – технологія навчання, коли основне засвоєння нового матеріалу відбувається самостійно, а час аудиторної роботи виділяється на виконання завдань, вправ, проведення лабораторних і практичних досліджень, індивідуальних консультацій. Таким чином, традиційне представлення лекції перевтілюється в її обговорення, у якому розкриваються дискусійні питання, презентуються проекти, виконуються практичні роботи тощо, а відео-лекція при такому підході стає ключовим компонентом (*Приходькіна, 2014*);

– **відкриті освітні ресурси** (Open educational resources, OER) – одна з розробок відкритої освіти (open education) у вигляді цифрових навчальних матеріалів, які знаходяться у вільному доступні в Інтернеті; викладачі та студенти можуть безкоштовно завантажувати та, за необхідності, адаптувати чи змінювати відповідно до ліцензії Creative Commons, яка забезпечує захист для творців матеріалу;

– **масові відкриті онлайн-курси** (MOOC) – інтернет-курси з масштабною інтерактивною участю та відкритим доступом через інтернет. На додаток до традиційних матеріалів навчального курсу, такі як відео, читання, і домашні завдання, MOOC надає можливість використання інтерактивної взаємодії користувачів, які допомагають створити спільноту студентів, викладачів та асистентів. Для MOOC характерна відкрита та проста реєстрація, великі обсяги аудиторії (від 1000 до 100 000), вільний доступ до відеозаписів лекцій, комп’ютерне оцінювання з моментальним зворотнім зв'язком.

Існують два принципово різні типи MOOCs (*Fidalgo-Blanco et al., 2016*):

1. **xMOOC** – це класичний курс на основі платформ е-навчання, в якому є початок і кінець, є лекції, інтерактивні тести та розділ для інтерактивного обговорення. Тут студенти мають дотримуватися термінів виконання завдань. Тобто xMOOC орієнтуються на більш традиційний, академічний підхід до освоєння матеріалу.

2. **cMOOC** ("c" – connectivism) – курси по принципу соціальних мереж, які засновані на спілкуванні учасників та обговоренні певних тем. Підхід базується на теорії з'єднувальних знань (connective knowledge). Це передбачає мережеву взаємодію та використання технологій Web 2.0 для пошуку знань, навчальних спільнот та

людей зі подібними інтересами, щоб створювати та розвивати різні сфери знань. Тут викладач стає модератором, який заохочує подібні контакти та самостійно збирає та аналізує, акумулює, розшарює зібраний матеріал. Такий підхід має більшу гнучкість і чутливість, а також забезпечує соціалізацію учасників – пошук однодумців та можливість розширення мережі контактів.

Одним з ефективних способів організації гібридного та онлайн навчання є створення відео-лекцій. Це дозволяє зробити лекційний матеріал доступним для повторного перегляду у будь-який час. Створення відео-лекцій може відбуватись:

– проведенням автоматичного запису лекцій, які проходять в аудиторії, щоб студенти могли повертатись до проведених занять;

– попередній запис лекції для того, щоб студенти дивилися їх самостійно з наступним обговоренням в аудиторії.

Для підготовки відеоматеріалу лекцій про гібридні загрози слід звернути увагу на практику створення **TED-лекцій (TED Talk)**. Організатори збирають TED-конференції, щоб просувати ідеї, які мають змінити світ. Специфіка формату TED-лекцій привернула увагу всього світу та зробила їх окремим явищем просвітництва:

– в якості спікерів запрошують найяскравіших особистостей (вчених, філософів, музикантів, меценатів, бізнесменів тощо);

– спіч-лекція триває не більш ніж 18 хвилин, протягом яких доповідачі мають донести своє послання аудиторії, що зібралася; лекція має бути не просто цікавою – вона має надихати та захоплювати;

– ці натхненні виступи можна дивитись не лише наживо: їх транслюють онлайн, записують та викладають у мережу для безкоштовного використання на платформі TED.com;

– обов'язковим є супровід слайдами / субтитрами із базовими визначеннями, класифікаціями і т.п., що надає можливість одночасно і слухати, і читати;

– до кожного відео надається не лише список літератури, а ще й перелік посилань на фільми, події, історії, які ілюструють матеріал.

Важливо зазначити, що який би підхід не обирав лектор, діяльність викладача на всіх етапах підготовки й проведення лекцій має орієнтуватися на логіку сучасних дидактичних технологій. Формат лекцій залежить від:

– прогностичності цілей навчання (чому навчати і для чого навчати?);

– з урахуванням рівня кваліфікації викладача (хто навчає?);

– особливостей аудиторії (кого навчає?);

– відбору і проектування змісту освіти (який саме матеріал давати?);

– форм організації навчального процесу (як навчати?);

– методів і засобів навчання (за допомогою чого?);

– діагностики досягнутих результатів (що вийшло?).

Саме такі підходи дозволяють найбільш виважено і раціонально використовувати таку форму навчання, як лекції, що за своїм рівнем відповідають вимогам підготовки висококваліфікованих фахівців.

Джерела посилань

Bates, A. W. (2015). Teaching in a digital age: Guidelines for designing teaching and learning. BCcampus.

Fidalgo-Blanco, Á., Sein-Echaluce, M. L., García-Peñalvo, F. J. (2016). From massive access to cooperation: lessons learned and proven results of a hybrid xMOOC/cMOOC pedagogical approach to MOOCs. International Journal of Educational Technology in Higher Education, 13 (1). doi: https://doi.org/10.1186/s41239-016-0024-z

Приходькіна, Н. О. (2014). Використання технології "переверненого" навчання у професійній діяльності викладачів вищої школи. Науковий вісник Ужгородського національного університету. Серія: Педагогіка. Соціальна робота, 30, 141–144. Available at: http://nbuv.gov.ua/UJRN/Nvuuped_2014_30_53

3. ПРАКТИЧНЕ ЗАНЯТТЯ

Світлана Гришко[1]
Ольга Копієвська[2]
[1]Харківський національний університет радіоелектроніки
[2]Національна академія керівних кадрів культури та мистецтв

Перенесення центру ваги на практичні заняття у навчанні є загальною тенденцією сучасності (*Bates, 2015; p. 168*). Але навчання в умовах гібридних загроз робить принципово важливим не пасивне споживання інформації, а саме активне залучення студентів до опрацювання матеріалу та застосування його в різних практичних ситуаціях.

Специфіка гібридних загроз вимагає надання студентам навичок:

– прийняття рішень як в зрозумілих ситуаціях, так і в аномальних;

– роботи індивідуально та в групі, формування навичок соціальних комунікацій для вирішення проблем;

– роботи в умовах запасу часу та дефіциту часу.

Такі навички формуються під час практикування активних дій. Тому різні форми практичних занять є невід›ємним елементом навчання в умовах гібридних загроз.

Протидія гібридним загрозам, які націлені на механізми прийняття рішень, вимагає когнітивного захисту. Це означає, що студенти мають навчитись самостійно добувати або конструювати знання на основі академічних критеріїв, таких як логіка, докази та аргументи. Розвиток критичного мислення вчить студентів думати про світ по-іншому. Для досягнення таких завдань важливе значення мають **розмова та обговорення**. Важливо, щоб студенти навчались через взаємодію та обговорення між собою, щоб отримати навички побудови соціальних контактів через поєднання власних

індивідуальних інтересів з інтересами інших учасників. Навчання, яке відбувається через діалог, має стати невід›ємним елементом на курсах з протидії гібридним загрозам.

Діалогічне навчання (dialogical learning) – це навчання через діалог, в якому різні люди надають аргументи, засновані на претензіях на обґрунтованість, а не на владу (*Kincheloe & Horn, 2007, p. 552*). Різноманіття форм діалогічного навчання дозволяє підібрати ті аргументи, які відповідають специфіці та завданням конкретного навчального процесу, наприклад:

– **семінарські заняття:** це форма навчання, під час якої студенти обговорюють матеріал, який був викладений на лекції, у групі під керівництвом викладача;

– **дискусії:** під час дискусій студенти висловлюють свої думки щодо певної проблеми або теми, інколи під час цього процесу можуть змінювати своє ставлення до певної теми;

– **суперечливі дискусії:** це форма діалогічного навчання, під час якої студентам пропонується висловити свої аргументи "за" та "проти" певної тези, що дозволяє розвивати навички аргументації та доказовості;

– **круглий стіл:** це форма діалогічного навчання, під час якої студенти засідають за круглим столом і обговорюють певну тему, обмінюються думками.

Іншою невід'ємною складовою курсів з протидії гібридним загрозам має стати забезпечення практичної активності студентів, яка забезпечується різними підходами:

– "**навчання через дію**" (Learning by doing) базується на тому, що найбільш ефективним способом навчання є активна участь студентів у практичних завданнях, дослідженнях та інших формах практичного досвіду. Навчання відбувається як осмислення власного досвіду, особливо того досвіду, де студенти беруть активну участь у створенні речей і дослідженні світу (*Bruce & Bloch, 2012*);

– "**навчання на основі проблем**", проблемно-орієнтований підхід (Problem-based learning) – передбачає вирішення студентами реальних проблем, які виникають у певній області знань, та допомагає розвивати їхні навички самостійного пошуку інформації та аналізу, а також попрактикуватись у розв'язанні реально

існуючих проблем. До того ж вирішення реальних проблем дає відчуття відповідальності. Але й слід врахувати, що для студентів цей підхід може виявитись складним, якщо їх база знань недостатня, та призвести до "когнітивного перевантаження" (cognitive overload);

– "**навчання на основі кейсів**" (Case-based learning) – використовує реальні або вигадані сценарії, щоб допомогти студентам зрозуміти теорію та її практичні застосування. Студентам пропонується аналізувати та розв›язувати проблеми, що виникають у цих сценаріях.

Існує велика кількість підходів до **навчання через дію** (Learning by doing), серед яких можна визначити наступні:

– **лабораторні роботи, робота в майстерні або студії:** студенти отримують можливість виконувати практичні завдання та дослідження у контрольованому середовищі, що надає їм можливість побачити теорію "в дії", перевірити гіпотези та впевнитись, наскільки добре працюють концепції, теорії чи процедури. Це можуть бути різні формати, наприклад:

1) "**мокрі лабораторії**" (Wet labs) – лабораторні заняття, де студенти працюють з реальними зразками та речовинами (звідси й назва), використовуються, зазвичай, при навчанні природничих наук, зокрема біології, хімії та фізики, для проведення експериментів (аналіз проб рідин, культивування мікроорганізмів, синтезу речовин, тестування нових матеріалів тощо). Wet labs вимагають спеціального обладнання та матеріалів, а також від студентів дотримання правил безпеки;

2) **віддалені лабораторії** (Remote labs) – дозволяють студентам проводити експерименти та дослідження за допомогою віддаленого доступу до реального обладнання, яке знаходяться в іншому місці, або симуляцій. Це вимагає використання веб-камер, мережевого з'єднання, відеоконференцій, програмного забезпечення для збору даних, спеціального фізичного обладнання тощо.

З точки зору протидії гібридним загрозам, важливо, що лабораторія (студія, майстерня) знайомить студентів із критично важливим культурним аспектом науково-технічного дослідження: всі ідеї мають бути перевірені суворим і особливим чином, щоб їх верифікувати (вважати істинними);

– **практика** у реальному середовищі: студенти отримують можливість **спостерігати** за процесами та вчитися розв'язувати проблеми, що виникають в реальному житті;

– **стажування:** студенти отримують можливість **працювати** у реальному середовищі, знайомитися з певною галуззю, брати участь у робочому процесі та у вирішенні проблем, що виникають у роботі;

– **змагання та конкурси:** студенти можуть брати участь у суперницькій взаємодії, де вони можуть використовувати свої знання та навички для конкурентного вирішення завдань та проблем;

– **рольові ігри та симуляції:** студенти грають ролі та вирішують завдання, які схожі на ті, що можуть зустрітися у реальному житті, що дозволяє їм навчитися приймати рішення та розв›язувати проблеми у непередбачуваних ситуаціях.

В умовах гібридних загроз набувають актуальності такі **форми роботи студентів**:

– **групові** проекти та завдання, спільне навчання (cooperative learning) передбачають, що студенти об'єднуються, обговорюють ситуацію та вирішують проблеми спільно (*Dishon & O'leary, 1984*). Це допомагає розвивати навички взаємодії, співпраці та комунікації. Це може також сприяти розвитку навичок стійкості та пильності, оскільки студенти мають виконувати завдання у межах визначеного часу та зосереджуватись на досягненні спільного результату;

– вправи на **розвиток уваги та концентрації**, які можуть бути організовані окремо або включені до різних типів занять;

– **гейміфікація** – включення елементів ігрового дизайну в освітнє середовище (*Dichev & Dicheva, 2017*). Елементами гейміфікації є таблиці лідерів, нагородні бали, значки, наклейки тощо. Гейміфікація збільшує участь, залучення та конкуренцію. Гейміфікація стимулює учнів до навчання та практикування, створює інтерактивне середовище в аудиторії та спонукає студентів щоразу працювати краще.

Більш складною формою практичного навчання студентів є **«Навчання на основі проектів», проєктно-орієнтована (Project-based learning)** форма навчання, де студенти отримують можливість вести наукові дослідження та виконувати проєкти, які вимагають від них застосування *комплексу різних знань та навичок*,

щоб дійти до певного результату (*Project Based Learning, n.d.*). Така міждисциплінарність є корисною практикою в умовах гібридних загроз, які також характеризуються мультидоменністю та мульти-інструментальністю.

Крім того, "Навчання на основі проєктів" сприяє розвитку сукупності аналітичних, дослідницьких та презентаційних навичок. Під час роботи над проєктом, студенти працюють у команді та вирішують реальні проблеми, що вимагають пошуку інформації, аналізу, дослідження та створення конкретного продукту або рішення. А створення проєктів, які потребують довготермінового планування та виконання, допоможе студентам розвивати навички пильності, витривалості та терпіння.

Допоміжним методом навчання студентів у складних непередбачуваних умовах гібридних загроз може стати наставництво.

Наставництво (mentorship, apprenticeship) – це процес, у якому більш досвідчений наставник допомагає менш досвідченому учню у розвитку його знань та навичок. Цей підхід може використовуватися у комбінації з іншими методами навчання та забезпечує індивідуальний підхід до кожного студента.

Викладачеві під час **організації практичних завдань та занять** в умовах гібридних загроз важливо звернути увагу на низку особливостей:

1. Орієнтація на потреби студентів: знаходження у сфері того, чим живуть студенти, забезпечить максимальну увагу та зацікавленість під час практичних вправ та користь від навчання.

2. Активна участь студентів: залучення до вирішення практичних завдань, взаємодії з іншими студентами, обговорення проблем та пошук їх рішень стає обов›язковою умовою навчання в умовах гібридних загроз, тому викладачеві потрібно забезпечити таку залученість через присутність, доступ студентів до технологій, ресурсів (мається на увазі як онлайн-технології навчання, так і технології, які вивчаються під час занять).

3. Фокус на практичному застосуванні знань: теоретичний матеріал має допомагати студентам застосовувати отримані знання на практиці, надавати можливість практикувати нові навички та отримувати фідбек від викладачів.

4. Використання сучасних технологій: інтерактивні технології, онлайн-інструменти, симуляції допомагають підвищити ефективність практичних занять та зробити їх більш захоплюючими та динамічними.

5. Оцінка результатів: всі практичні заняття, вправи та завдання повинні мати ясні цілі та визначені критерії оцінювання, які дозволять визначати об›єктивні результати, відстежувати прогрес студентів та забезпечувати регулярний контроль їх роботи. Це – важливий стимул для досягнення цілей навчання та розвитку навичок стійкості та пильності.

Джерела посилань

Bates, A. W. (2015). Teaching in a digital age: Guidelines for designing teaching and learning. BCcampus.

Bruce, B., Bloch, N.; Seel, N. M. (Ed.) (2012). Learning by Doing. Encyclopedia of the Sciences of Learning. Boston: Springer, 1821–1824. doi: https://doi.org/10.1007/978-1-4419-1428-6_544

Dichev, C., Dicheva, D. (2017). Gamifying education: what is known, what is believed and what remains uncertain: a critical review. International Journal of Educational Technology in Higher Education, 14 (1). doi: https://doi.org/10.1186/s41239-017-0042-5

Dishon, D., O'leary, P. W. (1984). A Guidebook for Cooperative Learning: A Technique for Creating More Effective Schools. Holmes Beach: Publication Sales, Learning Publications, Inc.

Kincheloe, J. L., Horn, R. A. (Eds.) (2007). The Praeger handbook of education and psychology. Vol. 4. Greenwood Publishing Group.

Project Based Learning. Available at: https://www.pblworks.org/what-is-pbl

4. ВОРКШОП ТА МАЙСТЕР КЛАС

Тетяна Борозенцева[1]
[1]Горлівський інститут іноземних мов

Майстер-клас та воркшоп є двома різними форматами навчальних заходів, які часто використовуються для передачі знань та навичок у практичний спосіб.

Воркшоп зорганізується та проводиться як практичне дослідження, що зосереджене на окремій та неоднозначній проблемі і здійснюється групою людей, зусилля яких певним чином організовані; це дозволяє розглянути проблему цілісно, під різними, нестандартними кутами зору (**табл. 1**).

Завдання воркшопу:

– допомогти актуалізувати досвід, наявний в учасників групи;

– спираючись на наявні ресурси, інтегрувати нову позицію розуміння та аналізу проблеми, що розглядається групою;

– покращити здатність учасників розв'язувати подібні проблеми.

Принципи роботи у форматі воркшопу:

– залучення учасників до активної співпраці та самостійного пошуку рішення проблеми;

– миттєвий зворотній зв›язок (бути завжди поряд с учасниками);

– заохочення розбіжності у думках, мотивація студентів вчитися один у одного;

– підтримка шанобливої форми висловлювання критичних суджень.

Майстер-клас передбачає попередню демонстрацію ведучим практичних прийомів та методів вирішення проблем за означеною тематикою, організацію процесу відпрацювання запропонованих практичних технологій в індивідуальному чи груповому форматі та

обговорення результатів роботи (*Єрмола & Василенко, 2006*). У якості ведучих долучаються партнери-експерти, які мають практичний досвід вирішення питань, пов'язаних із запобіганням гібридних загроз в окремій сфері.

Таблиця 1. Структура воркшопу

Назва етапу	Завдання	Результат етапу
Вступна частина	Знайомство учасників, обговорення правил роботи, регламенту. Оголошення теми, мети, очікувань та критеріїв результату заняття	Створення невимушеної атмосфери для навчання (відкритість для запитань та пропозицій)
Інформаційна частина	Надання актуальної та практичної інформації стосовно запланованої теми обговорення. Постановка проблеми	Введення учасників у розуміння проблеми. Створення зацікавленості у її розв'язанні
Практична частина	Організація процесу самостійного пошуку рішення проблеми (робота в малих групах, загальна дискусія, брейншторм тощо)	Знаходження оригінальних ідей, корекція та консолідація точки зору учасників
Підбиття підсумків	Узагальнення змістовних результатів роботи. Зворотній зв'язок від учасників	Емоційне підкріплення набутого досвіду з теми навчання

Головне завдання майстер-класу – узагальнити та поширити розроблену авторську технологію за проблематикою протидії гі-

бридним загрозам. В процесі навчання йде безпосереднє обговорення запропонованого методичного продукту та апробація його використання учасниками заняття.

Приклад тематики майстер-класу (*Данилюк, 2021; Freedman et al., 2021; Mazaraki et al., 2021*):

– техніки аналізу засобів та заходів ідеологічної дезорієнтації та розкладання свідомості певних груп людей з метою зниження їх ідейної, політичної, духовної та морально-психічної стійкості;

– прийоми запобігання інструментам впливу ворожих спецслужб (компрометація, дезінформація, науково-технічна розвідка та розвідка у ЗМІ противника, агентурне проникнення, вербування);

– технології викриття дезінформації, яка використовується для дестабілізації суспільства шляхом прямих атак на цивільні території та спроб спровокувати поляризацію та заворушення;

– методика виявлення підривної діяльності на основі розвитку мережі спеціалістів центральних органів державної влади у кожній сфері державного управління та суспільного життя та ін.

Методика проведення майстер-класів здебільшого не має єдиних норм і залежить від рівня інтуїції провідного фахівця і ступеню сприйнятливості слухачів. При цьому хід майстер-класу повинен спиратись на певну структуру, яка гарантує якісне виконання завдань заходу, а саме: відтворення ведучим власної технології в тематиці протидії гібридним загрозам; навчання учасників майстер-класу конкретним навичкам, що становлять основу транслььованого аналітичного досвіду; популяризація інноваційних ідей, авторських знахідок в означені сфері; надання допомоги учасникам майстер-класу у визначенні завдань їх власного подальшого самовдосконалення в напрямі опанування технології запобігання гібридним загрозам.

Активізація пізнавальної діяльності учасників майстер-класу, ефективне практичне освоєння найважливіших навичок у рамках демонстрованого досвіду забезпечується:

– виразністю інноваційної ідеї майстер-класу та культурою її презентації ведучим;

– вибором, повнотою, прогресивністю та оригінальністю запропонованої технології;

– здатністю мотивувати до включення кожного учасника в активну творчу роботу зі створення нового продукту діяльності на занятті;

– технологічністю запропонованих процедур аналізу інформації та синтезу нових ідей, етапів самоаналізу та самокорекції дій учасниками майстер-класу;

– загальною ерудицією та культурою спілкування ведучого, нестандартністю мислення, здатністю до імпровізації.

Воркшоп і майстер-клас базуються на одному тому самому принципі – "навчання через практику". Але, як бачимо, вони по різному реалізують цей принцип у навчальному процесі.

Майстер-клас проводиться одним або кількома експертами, фокусується на демонстрації та показі певних технік, методів або процесів у практичній формі, де учасники досить пасивно спостерігають, сприймають запропоновану інформацію та демонстрацію від експерта, і потім залучаються до практичного відтворення презентованого досвіду, готової технології.

Воркшоп також проводиться експертами, але він передбачає активну роботу учасників, має інтерактивний характер, спрямований на взаємодію та вирішення конкретних завдань або проблем. На відміну від майстер-класу, учасники воркшопу активно залучаються до творчої діяльності, яка передбачає креативний пошук шляху виконання практичних завдань.

Ще однією відмінністю можна вважати регламент занять: майстер-клас завжди має чіткий початок та завершення демонстрації тієї чи іншої технології, а воркшоп може надавати студентам можливість долучатись до виконання практичних вправ у будь-який зручний момент (за аналогією з майстернею, де людина має змогу творити будь-коли).

Таким чином, майстер-клас має на меті познайомити учасників з конкретними технікам або прийомами, а мета воркшопу – сприяти практичному навчанню та формуванню практичних навичок, обміну досвідом, створенню нових ідей та спільному вирішенню проблем.

Воркшоп та майстер-клас можуть поєднуватись під час організації занять, створюючи велику кількість різноманітних гібридних форм для навчання через практику.

Джерела посилань

Freedman, J., Hoogensen Gjørv, G., Tahinjanahary Razakamaharavo, V. (2021). Identity, stability, Hybrid Threats and Disinformation. Revista ICONO14 Revista Científica de Comunicación y Tecnologías Emergentes, 19 (1), 38–69. doi: https://doi.org/10.7195/ri14.v19i1.1618

Mazaraki, A., Kalyuzhna, N., Sarkisian, L. (2021). Multiplicative effects of hybrid threats. Baltic Journal of Economic Studies, 7 (4), 136–144. doi: https://doi.org/10.30525/2256-0742/2021-7-4-136-144

Данилюк, О. В. (2021). Методика раннього виявлення гібридних загроз в умовах агентурних заходів впливу РФ. Актуальні Проблеми Політики, 67, 135–142. doi: https://doi.org/10.32837/app.v0i67.1164

Єрмола, А. М., Василенко, О. М. (2006). Технологія організації науково-методичної роботи з педагогічними кадрами. Харків: Курсор, 312.

5. БРЕЙНШТОРМ ТА СИМУЛЯЦІЯ

Павло Худ[1]

[1]Український католицький університет

Брейншторм

Брейншторм є одним із методів сприяння груповій креативності, за допомогою якого учасники спонтанно обмінюються ідеями та думками з метою прийняття рішень (*Al-Samarraie & Hurmuzan, 2018; Gogus, 2012*).

Особливістю методики брейншторму є те, що вона дозволяє усім або максимальній кількості учасників висловити своє бачення стосовно якоїсь вже існуючої ідеї чи теми.

Брейншторм важливий, коли у вас є уявлення про бажаний результат, але не видно чіткого рішення. Саме у такій ситуації є сенс використовувати брейншторм як навчальну методику, щоб разом із студентами подумати над різноманітними, навіть божевільними ідеями, поки ви не знайдете те, що працює (*Roth, 2015*).

Помилкою є використання брейншторму на етапі генерування нових ідей, через що ця методика може виглядати хаотичною і часто від неї відмовляються. Через це, техніка мозкового штурму перетвориться на простір перекрикування один одного, суперечки щодо того, чия думка правильна, а чия неправильна. У підсумку зростає ризик того, що буде ухвалено абсурдне рішення, або запропоновано абсурдну ідею (*Кнапп et al., 2016*).

Брейншторм є інструментом, який можливо добре використовувати у процесі прийняття рішення. Він складається з трьох компонентів: генерування ідей для нових рішень, тестування ідей нових рішень та впровадження нових ідей, щоб знайти найбільш оптимальне рішення.

Методика брейншторму застосовується на етапі тестування ідеї. Окрім брейншторму, у процесі тестування ідей також можна використовувати методику прототипування. На етапі тестування ідеї важливо бути скептичним до висловленої напередодні ідеї. Брейншторм має допомогти з'ясувати, що потрібно змінити в ідеї, щоб вони стала ще кращою та ефективнішою.

При формуванні команд для брейншторму важливо звернути увагу на те, щоб до її складу увійшли учасники з різним досвідом та знаннями. Завдяки цьому учасники брейншторму зможуть надбудовувати нові ідеї на основі існуючих, а не сперечатися між собою, чия ідея краща.

Важливо, щоб під час занять викладачі створили атмосферу, коли думки студентів довкола запропонованих раніше ідей допомагали створювати нові рішення, хоч якими б дивовижними вони не здавалися у момент обговорення.

Ніхто з учасників брейншторму не повинен вдаватися до оціночних суджень щодо ідей інших учасників. Викладачі як фасилітатори брейншторму мають спостерігати за тим, щоб учасники залишалися у просторі обговорюваної теми, не переходили на обговорення інших тем та діяв принцип: коли один говорить, інші мовчать.

Ще одним підхід до ефективного використання методики брейншторму можна назвати Модель 6-3-5 (*Markman, 2017*). Для цього поділіть студентів на команди по шість осіб і посадіть кожну команду за окремий стіл. Попросіть кожного учасника команди написати три ідеї і передати їх тому, хто сидить праворуч.

Таке переміщення зробіть п'ять разів, щоб усі учасники команди могли побачити ідеї інших, пропозиції інших та додати свої думки. Після цього запропонуйте учасникам обговорити всі ідеї разом за одним столом. Хоч цей процес займе більше часу, проте дозволить висловитися всім учасникам команди та запропонувати свої ідеї.

Посилання на додаткові ідеї щодо організації брейншторму можна знайти у переліку посилань (*Markman, 2019; Markman, 2020; Tsipursky, 2022; Gregersen, 2018; Besieux et al., 2021; Rogelberg & Kreamer, 2019*).

Симуляція

Для перевірки знань студентів викладачі можуть використовувати навчальний метод "симуляційна гра". Цей метод допомагає студентам приймати рішення в аудиторії, тестуючи варіанти рішень для ситуацій, що відбуваються в умовах реальних життєвих обставин.

За допомогою симуляційної гри у студентів випрацювується аналітичне мислення і вони краще можуть описувати результати своїх спостережень. Працюючи з кейсами за допомогою симуляційної гри студенти мають змогу показати свої сильні індивідуальні сторони та свою команду, показати спроможність і внесок, який робить кожен із них в результат команди.

Методика симуляції належить до категорії **експериментального навчання** (experiential learning). Ця методика допомагає працювати з неправильними уявленнями студентів про явища та події (*McClintock, 2000*), розвиває здатність до критичного мислення (*Kreber, 2001*) та самостійного навчання (*Hakeem, 2001*) і допомагає студентам краще зрозуміти предмет.

Метод симуляційна гра можна використовувати при різних форматах навчання: онлайн, офлайн, чи змішаний онлан / офлайн формат. Значно важливішим за формат навчання, в якому ми хочемо провести симуляційну гру, є вибір симуляційної моделі, за допомогою якої слід перевірити знання студентів. Насамперед, слід обрати симуляційну гру, яка найкраще відповідає дисципліні, яка читається студентам.

Серед форм симуляційного навчання є техніка моделювання, під час якої студенти мають змогу вчитися один в одного (*Dorn, 1989*). Навчання відбувається через активну залученість кожного учасника навчального процесу, а не пасивного слухання по лінії "викладач навчає – студент слухає".

Моделювання як симуляційну практику можна застосовувати при вивченні таких тем як економіка торгівлі та економіка бідності, розвиток та становлення бізнесу, вивченні практик сімейного життя та подружньої взаємодії (*Osmond, 1979*), міжлюдської взаємодії у соціальних науках та публічному управлінні (*Rocha, 2000*).

Якісне запровадження симуляції як навчальної методики передбачає три етапи: (I) підготовка, (II) залучення студентів, (III) підсумки.

Підготовка

На етапі підготовки симуляційного завдання важливо зрозуміти, які цілі курсу і наскільки симуляційна техніка дозволяє їх досягнути. Перш, ніж застосовувати її безпосередньо на занятті, слід зробити пробний запуск. Ефективність застосування симуляційної методики тісно корелюється з рівнем активності студентів. Через це слід зважати на кількість студентів на заняття, оскільки для кожного з них має бути своя роль і ніхто із студентів не має залишитися пасивним учасником симуляційного навчання.

Для використання симуляційної техніки також має значення приміщення, в якому вона проводитиметься. Важливо, щоб симуляційна методика поєднувалася з іншою навчальною методикою, а не була єдиною, яку застосовує викладач на занятті. Оскільки щось може піти не так, викладач має також перестрахуватися, що він робитиме у такому випадку. Для максимального залучення аудиторії корисно використовувати онлайн-ресурси, відповідну інформацію можна знайти в **табл. 2**.

Залучення студентів

Симуляційне навчання ефективне при умові, що студенти активно включені у процес навчання. Викладачі мають докласти зусилля до того, щоб усі студенти були активно включені. Активність студентів зростає за умови, коли вони перед її проведенням намагаються передбачити та пояснити результати симуляційного навчання, а також коли кожен з них обирає для себе якусь роль у процесі проведення симуляції.

Підсумки

Обговорення після проведення симуляційного навчання дозволяє студентам закріпити знання та розширити простір для можливого їх застосування. Для цього у студентів має бути достатньо часу, особистої рефлексії та групового обговорення.

Важливо, щоб викладачі підготували запитання, які допоможуть студентам зістикувати між собою симуляційну практику та навчальні цілі.

Релевантною симуляційною грою у контексті проекту Erasmus WARN з виявлення та протидії гібридним загрозам може бути кейс IT-менеджмент симуляцій: гібридна атака. "Ця симуляційна гра

навчає студентів ключовим проблемам, з якими стикаються менеджери, реагуючи на ІТ-кризу. Виконуючи роль технічного директора у компанії в розпал кібератаки, студенти навчатимуться визначати пріоритети та приймати обґрунтовані рішення, які посилюють збереження даних. Вони орієнтуватимуться на складнощі спілкування у швидко плинному середовищі, водночас дізнаючись про важливість готовності до кризи.

У першій частині симуляції студенти зіткнуться зі сплеском інформації, суперечливими думками та низкою подій, які вони повинні діагностувати, на які повинні реагувати та після якої мають відновитися. У другій частині симуляції студентам буде доручено написати публічну заяву про напад, а потім переглянути заяви інших учасників симуляційної гри" (**табл. 4, п. 1**).

Симуляція відмінна від гри і не передбачає, що хтось буде переможцем. Вона також відмінна від методі кейс-стаді, оскільки не передбачає можливості дивитися на проблематику ззовні та зсередини.

Один із важливих елементів симуляції (на відміну від гри чи кейс-стаді) полягає у тому, що кожен учасник повинен обрати для себе свою роль і намагається вирішити проблему через подію, в якій він приймає участь.

Переваги симуляційного навчання у тому, що студенти не лише навчаються, але особисто, через певну роль у події, здобувають свій досвід.

Симуляційна методика може також не виконати свого призначення. Це можливе принаймні з трьох причин: студенти не підготовлені, у процесі симуляції студенти захоплюються певним її елементом або акцентують увагу саме на ньому. Або ж, студенти відхиляються від навчальної цілі, передбаченої курсом.

Щоб уникнути ризику непідготовленості, можна завчасно запланувати, щоб певні ролі взяли на себе студенти, які досягнуть результату. Також не слід боятися повертати студентів до основної цілі симуляційної методики.

Зазвичай симуляційну гру найкраще проводити всередині семестру, тому що вже пройде достатньо часу для вивчення матеріалу, який викладач зможе оцінити на прикладі роботи з кейсом у симуляційній грі.

Таблиця 2. Симуляційні кейси у різних сферах

№	Автори	Назва ресурсу	Опис	Посилання
1	**2**	**3**	**4**	**5**
1	Robert D. Austin	IT Management Simulation: Cyber Attack!	Симуляція ролі технічного директора компанії в розпал кібератаки	https://hbsp.harvard.edu/product/8690-HTM-ENG
2	Центр викладання та навчання Advantexe	Симуляція ситуацій у бізнесі та втілення стратегічних ініціатив	Бізнес-симуляції: – Business Acumen / Ділова хватка – Business Leadership / Лідерство – Business Selling / Продаж бізнесу	https://www.advant-exe.com/
3	Центр наукової освіти UCAR	Осмислити науку про Землю за допомогою ігор та симуляції	Ігри та симуляції, пов’язані з погодою, кліматом, наукою про атмосферу тощо	https://scied.ucar.edu/interactive
4	Проєкт PhET Interactive Simulation в Університеті Колорадо	Інтуїтивно зрозуміле середовище, схоже на гру, в якому студенти вчаться, досліджують, роблять відкриття	Симулятори PhET засновані на освітніх дослідженнях в галузі: – Physics / Фізика – Chemistry / Хімія – Math / Математика – Earth Science / Наука про Землю – Biology / Біологія	https://phet.colorado.edu/

Продовження Таблиці 2

1	2	3	4	5
5	BBC	Сирійська подорож: виберіть власний шлях втечі	Якби ви тікали з Сирії, щоб ви зробили для своєї родини? Зрозумійте справжні дилеми, з якими стикаються біженці	https://www.bbc.com/news/world-middle-east-32057601
6	Розробка McKinney для Urban Ministries of Durham (США)	SPENT – онлайн-гра про бідність і безпритульність	Гравці мають приймати складні рішення в умовах бідності, щоб прожити один місяць на 1000 доларів, та часто змушені вибирати між однаково поганими варіантами (вибір між оплатою електроенергії та здоровою їжею) тощо	http://playspent.org/html/
7	Harvard Business Publishing	Помістити студентів прямо в контекст реалістичних бізнес-сценаріїв, де вони повинні застосовувати концепції, яким навчилися, щоб приймати рішення під тиском	Моделювання у різних дисциплінах: – Accounting / Бухгалтерський облік – Economics / Економіка – Entrepreneurship / Підприємництво – Finance / Фінанси – Management / Менеджмент – Information Technology / Інформаційні технології – Marketing / Маркетинг – Strategy / Стратегія тощо	https://hbsp.harvard.edu/simulations

Симуляції можуть працювати як індивідуальні чи групові проєкти, незалежно від розміру класу. Однак, щоб керувати часом уроку більш ефективно, слід розглянути можливість проведення симуляційної вправи як групового проєкту, у кожній групі не більше чотирьох учасників.

Джерела посилань

Al-Samarraie, H., Hurmuzan, S. (2018). A review of brainstorming techniques in higher education. Thinking Skills and Creativity, 27, 78–91. doi: https://doi.org/10.1016/j.tsc.2017.12.002

Besieux, T., Edmondson, A. C., de Vries, F. (2021). How to Overcome Your Fear of Speaking Up in Meetings. Harvard Business Review. Available at: https://hbr.org/2021/06/how-to-overcome-your-fear-of-speaking-up-in-meetings

Dorn, D. S. (1989). Simulation Games: One More Tool on the Pedagogical Shelf. Teaching Sociology, 17 (1), 10–18. doi: https://doi.org/10.2307/1317920

Gogus, A. (2012). Brainstorming and learning. Encyclopedia of the sciences of learning. Springer, 484–488. doi: https://doi.org/10.1007/978-1-4419-1428-6_491

Gregersen, H. (2018). Better Brainstorming. Harvard Business Review. Available at: https://hbr.org/2018/03/better-brainstorming

Hakeem, S. A. (2001). Effect of Experiential Learning in Business Statistics. Journal of Education for Business, 77 (2), 95–98. doi: https://doi.org/10.1080/08832320109599056

Kreber, C. (2001). Learning Experientially through Case Studies? A Conceptual Analysis. Teaching in Higher Education, 6 (2), 217–228. doi: https://doi.org/10.1080/13562510120045203

Markman, A. (2017). Your Team Is Brainstorming All Wrong. Harvard Business Review. Available at: https://hbr.org/2017/05/your-team-is-brainstorming-all-wrong

Markman, A. (2019). Bring Your Brain to Work: Using Cognitive Science to Get a Job, Do it Well, and Advance Your Career. Harvard Business Press.

Markman, A. (2020). How to Brainstorm – Remotely. Harvard Business Review. Available at: https://hbr.org/2020/07/how-to-brainstorm-remotely

McClintock, C. (2000). Creating Communities of Practice for Experiential Learning in Policy Studies. Social Change, Public Policy, and Community Collaborations, 33–51. doi: https://doi.org/10.1007/978-1-4615-4653-5_4

Osmond, M. W. (1979). The Use of Simulation Games in Teaching Family Sociology. The Family Coordinator, 28 (2), 205–216. doi: https://doi.org/10.2307/581676

Rocha, C. J. (2000). Evaluating Experiential Teaching Methods in a Policy Practice Course. Journal of Social Work Education, 36 (1), 53–63. doi: https://doi.org/10.1080/10437797.2000.10778989

Rogelberg, S., Kreamer L. (2019). The Case for More Silence in Meetings. Harvard Business Review. Available at: https://hbr.org/2019/06/the-case-for-more-silence-in-meetings

Roth, B. (2015). The achievement habit: Stop wishing, start doing, and take command of your life. New York: HarperCollins Publishing.

Tsipursky, G. (2022). Why Virtual Brainstorming Is Better for Innovation. Harvard Business Review. Available at: https://hbr.org/2022/02/why-virtual-brainstorming-is-better-for-innovation?utm_medium=email&utm_source=newsletter_weekly&utm_campaign=ascend_activesubs&deliveryName=DM185859

Кнапп, Дж., Зерацкі, Дж., Ковіц, Б. (2016). Спринт: Вирішуйте складні завдання і тестуйте нові ідеї за п'ять днів. Київ: ТАО.

6. ВАРГЕЙМІНГ: ВОЄННІ ІГРИ

Світлана Гришко[1]
Олександр Котуков[2]
[1]Харківський національний університет радіоелектроніки
[2]Харківський національний університет імені В. Н. Каразіна

Будь-яка спроба проаналізувати майбутнє спирається **на судження про невизначеність**. Особливо це стосується війни, яка є хаотичною і залежить від випадковості. Тому у сфері військового аналізу напрацьовані різні підходи до прийняття рішень в умовах складних та невизначених загроз.

Ці практики набувають актуальності **для цивільних спеціалістів в умовах гібридних загроз**, де розмивається межа між миром та війною, а зловмисник використовує військові принципи підходи і навіть інструменти в невійськових доменах для створення невизначеності та неідентифікованості. Але використання військових інструментів аналізу у цивільному освітньому процесі вимагає розуміння області та специфіки їх застосування.

Висока невизначеність військових конфліктів виникає через:

1) відсутність реальних даних для створення кількісних моделей, які б забезпечували статистичну достовірність;

2) неможливості кількісно оцінити такі ключові якісні чинники, як моральний дух і підготовка військ (*Cancian et al., 2023; с. 24*).

Ці проблеми характерні й для аналізу гібридних впливів. За цей час напрацьовані різні способи аналізу військових конфліктів, які спрямовані на зменшення вказаних типів невизначеностей:

1) **неструктуровані судження:** формування уявлення про хід подій на основі розуміння потужності збройних сил та за аналогією з епізодами воєнної історії;

2) **слабо структуровані судження:** прості кількісні порівняння (наприклад, чисельності збройних сил), яким бракує оцінки динамічної взаємодії;

3) **структуровані судження:** враховують комплекс критичних змінних, як-от:

– **планування місії** – моделювання параметрів METT-TC: Mission, Enemy, Terrain, Troops, Time, Civilians – Місія, Ворог, Місцевість, Війська, Час, Цивільні;

– **чиста оцінка** – це оцінка військових балансів за критичними напрямками;

4) **кількісні моделі** – це математичне представлення системи, як, наприклад, моделі **аналізу кампаній**: двосторонні моделі TACWAR та CEM для імітації бойових дій з розрахунком виснаження, які використовувались до 1990-х років; сучасні моделі військових кампаній (як JICM і STORM) тощо.

При аналізі у військовій справі історично існувало протиріччя між кількісним моделюванням та якісними судженнями. В ідеалі, аналіз конфлікту повинен поєднувати строгість і прозорість моделювання аналізу кампанії з людським фактором прийняття рішень. **Варгеймінг пропонує один з інструментів для поєднання цих двох підходів.** Саме ця важлива характеристика привертає увагу до воєнних ігор як до способу набуття навичок захисту в умовах гібридних загроз.

Варгеймінг (wargaming) не має єдиного загальноприйнятого визначення, наступні підходи якого відображають основні характеристики цієї практики:

– симуляція воєнних дій із використанням певних правил, даних, методів і процедур і зосереджена на рішеннях гравців, які впливають на послідовність подій (*NATO, 2022*); на **рис. 2** в ілюстративній формі представлена проблематика варгеймінгу, яку досліджують спеціалісти НАТО;

– модель воєнних дій, яка не залучає реальні сили, де на перебіг подій впливають рішення, прийняті під час цих подій гравцями, що представляють протиборчі сторони (*Perla, 1990*);

– техніка прийняття рішень на основі створення структурованого середовища, де можна вільно експериментувати, ризикувати

та здійснювати помилки, не страхуючись від негативних наслідків, щоб дослідити, що працює (перемога / успіх), а що ні (програш / невдача), як правило, за відносно низьку вартість (*DCDC, 2017; p. 5*);

– ігри, в яких люди приймають рішення в контексті конкуренції, конфлікту (*U.S. Naval War College, 2020*);

– структуровані розмови між експертами для прийняття рішень (*Vatne et al., 2022; p. 299*).

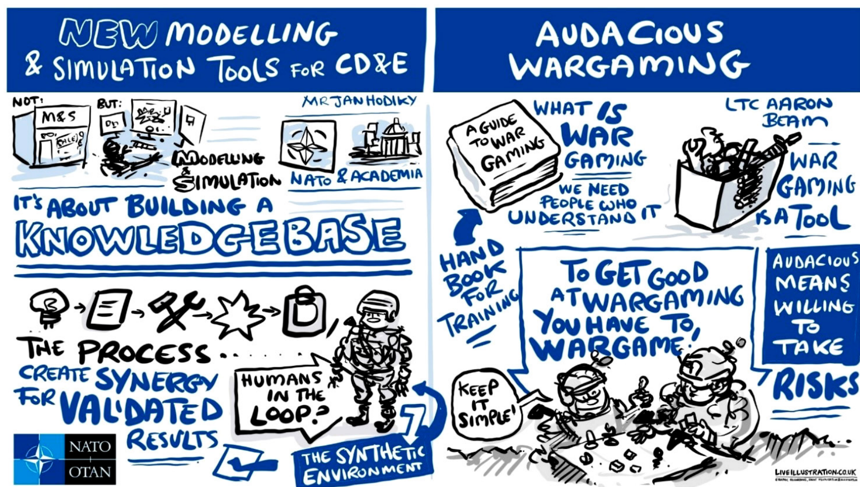


Рис. 2. Ілюстрація проблематики варгеймінгу, яка обговорювалась на міжнародній конференції CD&E (*NATO, 2022*), та розміщена на офіційній сторінці цієї конференції *https://www.act.nato.int/cde-conf*

Важливо, що варгеймінг стосується **конфліктних ситуацій**, де люди змагаються у **різних ролях**, приймаючи свої рішення як реагування на рішення інших гравців. З точки зору навчання протидії гібридним загрозам, важливо, що такі ігри підходять для **занурення учасників у середовище**, описане сценарієм, де вони піддаються різноманітним динамічним викликам і залежать від рішень інших учасників.

Організаційно варгеймінг – це процес креативного змагання, який подається у структурованому форматі та зазвичай здійснюється під керівництвом суддів. Він відбувається як певна динаміка подій, які створюються під впливом гравців. Поняття, які формують лексикон варгеймінгу, представлені в Додатку А.

Дизайн варгеймінгу складають такі елементи:

– мета і завдання: мають важливе значення для того, щоб проблема, яку необхідно розв'язати, була належним чином сформульована;

– дані та джерела: для створення установок та сценарію потрібна інформація, крім того, для моделювання потрібні кількісні параметри та дані;

– установки та сценарій, які забезпечують захоплююче середовище, у якому відбувається вся гра;

– допоміжний персонал та предметні спеціалісти – експерти, які допомагають створити гру та допомагають під час її проведення;

– гравці – діючі особи, які беруть на себе певні ролі, їх рішення створюють динаміку гри; кількість гравців може коливатися від одного до тисячі. Зазвичай вони організовані у групи, розмір і форма яких може значно змінюватися, має місце є кольорове кодування таких груп (див. додаток А);

– координатори (судді) – команда, що піклується про досягнення цілей гри, підтримує занурення гравців, виносить рішення (судить), модерує процес;

– симуляція, яка відбувається на основі створених установок, правил, процедур та критеріїв;

– аналіз – заснований на даних, зібраних у грі, дозволяє зрозуміти створений під час гри наратив, в основі якого спільний досвід гравців та уроки, які були отримані.

Складність елементів буде різною, але всі вони зазвичай присутні у варгеймінгу.

Воєнні ігри мають довгу історію у військовому аналізі та використовуються як педагогічні і дослідницькі інструменти в університетах, аналітичних центрах та урядових установах для вивчення питань безпеки – від кризової стабільності до регіональних конфліктів. В залежності від мети, воєнні ігри бувають (*Cancian et al., 2023; p. 26*):

1) **експериментальні** – мають на меті краще зрозуміти процес прийняття рішень людиною у конкретному контексті. Через маніпулювання ключовими змінними і запис дискусій, така гра дозволяє виявити варіанти розвитку подій;

2) **навчальні** – мають на меті сприяти підготовці лідерів до прийняття рішень на війні через моделювання вибору у складних умовах, при цьому виділяють:

– ігри, орієнтовані на "трансформацію себе", які надають військовим командирам **досвід** прийняття рішень;

– ігри, орієнтовані на поточні операції, які зосереджені на актуальній **інформації**, необхідній для прийняття рішень у даній ситуації;

3) **аналітичні** воєнні ігри, спрямовані на аналіз військових проблем у контексті всього спектру PMESII – доменів[1]. Для цього створюється аналітична архітектура, в якій будуються моделі на основі фактичних даних, потім розробляється дизайн гри, що перевіряється експертами у цій галузі; ця гра потім ітеративно розігрується невеликою групою людей для полегшення аналізу. Такий аналіз передбачає велику кількість ігрових ітерацій, варіативність сценаріїв і прийняття рішень на основі науково обґрунтованих правил.

Повний цикл військових досліджень об'єднують **воєнні ігри** ("маневри на карті"), **аналіз кампаній і військові навчання** ("польові маневри") для розуміння сценаріїв розгортання сучасної війни. Варгеймінг порушує питання, які потім досліджуються за допомогою військових навчань і математичного аналізу.

Застереженням до використання воєнних ігор є дотримання області використання: не слід плутати варгеймінг з конструктивним моделюванням – якщо варгеймінг був призначений для навчання учасників, але використовується як основа для аналізу, це призводить до марних зусиль і хибних висновків. Варгеймінг дозволяє моделям взаємодіяти в інтелектуальний спосіб. Конкретні події,

---

[1] PMESII – політичний, військовий, економічний, соціальний, інформаційний, інфраструктурний спектр. https://warn-erasmus.eu/glossary/pmesii/

з яких генеруються сценарії, є результатом інтелектуального прийняття рішень людьми-гравцями.

Кількісні результати створюють основу для якісних суджень про вплив однієї сфери на іншу.

При моделюванні варгеймінгу важливо **забезпечити наступні умови**:

1) збалансувати ступінь спрощення та кількість областей моделювання (наприклад, наземна, повітряна кампанії) та типів бойових дій;

2) визначити адекватні правила взаємодії, розподілу ресурсів та прийняття рішень, збалансувати складність та точність моделі;

3) сформувати:

– змінні – умови, які можуть вплинути на аналіз;

– сценарії – набори обґрунтованих припущень для кожної змінної;

4) забезпечити достовірність моделі: позначити, які області вимагають точності, а які можуть розглядатися абстрактно;

5) врахувати умову повноти моделі, включивши до неї всі критично важливі елементи: гра доречна лише тоді, коли обрані частини є єдиними значущими частинами конфлікту (наприклад, ракети класу "земля-повітря" є критично важливим елементом сучасного повітряного бою).

Мета гри – це не спроба дослідити всі можливі результати (це нереально), а спосіб оцінити основні лінії гри, які є результатом розумного прийняття рішень. Кожна ітерація дозволяє дослідити деякі з найбільш вірогідних варіантів розвитку подій, але одна ітерація не може проілюструвати загальні контури проблем. Повторне програвання сценарію з використанням різних стратегій необхідне, щоб недопустити помилкової орієнтації на стратегію, отриману з одного сценарію. **Ітерації виконують важливу роль** для створення висновків:

– ітерація у різних сценаріях з різними припущеннями щодо ключових змінних дозволяє провести аналіз чутливості;

– проводячи кілька ітерацій з одним сценарієм, а потім змінюючи сценарій, можна зробити висновки про важливість і вплив кожної зміни змінної.

Вибір **змінних** має відображати мету такої гри. Змінні повинні бути одночасно **невизначеними** і такими, що можуть мати **значний вплив** на результат. Вибір може ґрунтуватися на літературі або на уявленнях, отриманих під час гри (виявлення "невідомих невідомих").

Елемент **випадковості** (несподівана подія, шанс) досягається завдяки генератору випадкових чисел (гральні кубики, таблиці з інструментами, картки з подіями).

Активні, мислячі опоненти та елемент випадковості є основними засобами введення **невизначеності** у гру, однак можуть використовуватися інші методи:

– таємні рухи, поки розвідка їх не виявить;

– незрозумілі або невизначені цілі та наміри (включаючи цілі союзників);

– випадкові чинники сценарію (негода, технічна поломка, увага ЗМІ тощо);

– зміна послідовності гри, що може дозволити одній стороні зробити щось потайки або потрапити у процес прийняття рішень противника тощо.

Конкретний результат кожної ітерації не може передбачити майбутнє, але сам процес воєнних ігор є необхідним для аналізу конфлікту. **Будьте обережними**, граючи у варгеймінг, щоб не робити тверджень, які виходять за межі їх сфери застосування, і не плутати висновки воєнної гри з висновками їх моделювання.

Організація варгеймінгу може бути здійснена різними способами (*DCDC, 2017, p. 39–40; Vatne et al., 2022, p. 300*), основні з них представлені в **табл. 3**.

Варгеймінги є повторюваними і мають циклічний життєвий цикл:

1) проєктування; розробка;

2) проведення гри;

3) оцінка результатів та уточнення моделі.

Кожен етап вимагає ретельної підготовки (*DCDC, 2017, p. 51–60*).

Приклад організації варгеймінгу для спеціальності "Публічне управління та адміністрування" наведений у Додатку Б. Посилання на приклади організації варгеймінгу представлені в **табл. 4**.

Таблиця 3. Організаційні форми варгеймінгів

Форма	**Опис**
Ігри-семінари	Модеровані дискусії між людьми у спільному контексті / сценарії. Зазвичай мають вільну форму, носять дослідницькій характер, мають справу з відкритою інформацією. Гравців занурюють у контекст, просять приймати рішення, а потім обговорюють наслідки. Висновки ("Судові рішення") зазвичай є менш жорстким, але достатнім для просування перебігу подій. Винесення рішення може здійснюватися суддею або за консенсусом між гравцями. Зазвичай проводяться у малих групах. На відміну від звичайного семінару містить причинно-наслідкову взаємодію, змагальність та висновки про наслідки конкретних дій
Матричні ігри	Відбуваються за розподілом ролей та використовують формальні правила суддівства. Від гравців вимагається надати кілька конкретних аргументів на користь запропонованої дії, яка обмежена фантазією гравця або її реалізацією. Потім інші гравці можуть наводити контраргументи. Наступне коротке обговорення веде безпосередньо до результату винесення рішення. Дебати обмежені за часом, щоб дозволити кілька дій і протидій у грі. Тож учасники змушені жити з наслідками своїх рішень у наступних ітераціях. Модерують гру координатори / судді, які оцінюють аргументи "за" і "проти", та приймають рішення про ймовірність успіху курсу дій. Результат визначається киданням кубиків. Матричні ігри підходять для дослідження різних перебігів подій у контексті одного сценарію
Кригшпіль (Kriegsspiel)	Більш формальні воєнні ігри з підвищеним рівнем деталізації та суворості. Мають більш реалістичне уявлення про конфлікт із більш детальними сценаріями та представленням середовища

Таблиця 4. Опис прикладів організації варгеймінгу

№	Кейс	Опис	Посилання
1	Китайське вторгнення на Тайвань у 2026 році	Розробник: Центр стратегічних і міжнародних досліджень (CSIS), США Гра проведена у січні 2023 Чи вдасться китайське вторгнення? Які змінні впливають на результат? Якою буде вартість для обох сторін?	Cancian et al., 2023; p.40 – 160
2	Балтійський виклик	Розробник: Спільнота з дослідження військових операцій (MORS), USA; Tom Mouat (PAXsims). Гра проведена 17–20 жовтня 2016 Позиціонування сил НАТО / росії в Балтійському морі	http://www.mapsymbs.com/BalticChallenge.pdf
3	Kazhdyy Gorod	Розробник: Tom Mouat (PAXsims) Матрична гра "про місто колишньої радянської республіки Belaria на кордоні з росією, "січневу революцію" та протести"	http://mapsymbs.com/KazhdyyGorodSeriousMatrixGame.pdf

Джерела посилань

About wargaming. What is a war game? (2020). U.S. Naval War College. Available at: https://usnwc.edu/Research-and-Wargaming/Wargaming/About-Wargaming

Cancian, M., Cancian, M., Heginbotham E. (2023). The First Battle of the Next War. Wargaming a Chinese Invasion of Taiwan. A Report of the CSIS International Security Program. CSIS, 165. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/230109_Cancian_FirstBattle_NextWar.pdf

Perla, P. (1990). The art of wargaming. A guide for professionals and hobbyists. United States Naval Institute.

The Development, Concepts and Doctrine Centre (2017). Wargaming Handbook. DCDC. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

Vatne, D., Guttelvik, M., Hennum, A. C., Malerud, S. (2022). Wargaming for the Purpose of Knowledge Development: Lessons Learned from Studying Allied Courses Of Action. Scandinavian Journal of Military Studies, 5 (1), 297–308. doi: https://doi.org/10.31374/sjms.122

Wargaming the Future at the CD&E Conference. NATO. Available at: https://www.act.nato.int/cde-conf/cde-wargaming-future

8. ГРА В ДИЛЕМУ

Світлана Гришко[1]
Марія Головянко[1]
[1]Харківський національний університет радіоелектроніки

Для формування компетентностей з протидії гібридним загрозам можна використати підходи та методи антикризового управління.

Це пояснюється тим, що під час антикризового управління, так само як і в умовах гібридних впливів, відбувається прийняття "**складних рішень**", характеристиками яких є (*França & Borges, 2020*):

– стратегічний характер та високий рівень прийняття рішень, у результаті чого рішення піддаються впливам політичних міркувань, і тому стикаються з необхідністю узгодження розбіжних інтересів, а також вимагають сприйняття втручань населення (занепокоєння, недовіри, негативного впливу на політичну репутацію тощо);

– важливість: такі рішення впливають на розподіл важливих ресурсів та мають вирішальне значення для забезпечення життєдіяльності спільноти;

– ситуативність та контекстуальність (через унікальну природу кожної проблеми);

– когнітивна складність та високий рівень стресу, зокрема – й через ситуації "подвійного зв’язування" (double bind situations), коли менеджер отримує дві або більше суперечливих порад, одна порада з яких заперечує іншу;

– складні обставини – це динамічні та мінливі умови, невизначеність, неоднозначність, високі ставки, значні наслідки помилок, обмеження часу;

– міждисциплінарний характер, що ускладнює спільну ситуаційну обізнаність.

Велика частина невдач в управлінні кризою є результатом помилкового спільного усвідомлення ситуації (*DRIVER+ project, 2017; с. 12*). Особливо у тих випадках, коли вирішення проблеми має два та навіть більше варіантів, але жоден з них не є однозначно прийнятним чи кращим. Це вимагає зважування різних типів потенційних катастрофічних впливів, які необхідно пом'якшити (тобто **визначення пріоритетів**). Тому прийняття рішень в антикризовому управлінні часто стосується вирішення дилем.

Дилема – це ситуація, коли необхідно зробити важкий вибір між двома або більше альтернативами, які однаково небажані (*Oxford Reference*)

В умовах гібридних загроз, так само як і в антикризовому менеджменті, виникають дилеми. Коли **цінності людини входять у конфлікт**, створюються етичні, або ще гірше – моральні дилеми.

Етична дилема – це ситуація, в якій порушені правила життя конкретної особистості; вона зачіпає коло етичних питань: добро і зло, свобода та відповідальність, сенс життя, совість, обов'язок, щастя тощо

Найчастіше доводиться вибирати між тим, що правильно (з погляду моралі), але невигідні людині, – і тим, що погано для інших, але приносить особисту вигоду. У соціальних відносинах етична дилема – це, наприклад, безпека споживачів, права та дискримінація, професійна етика, корупція тощо.

Моральна (соціальна) дилема – це ситуація, в якій порушені норми моралі, тобто прийняті у суспільстві правила поведінки

Це – одна з найважчих ситуацій, в яку тільки можна потрапити. Необхідно вибрати один із взаємовиключних варіантів, причому обидва не принесуть нічого хорошого. Вирішення мораль-

них дилем розглядається у курсах логіки, конфліктології, психології, теорії ігор тощо. Існують загальновідомі постановки завдань: "дилема ув'язненого", "дилема секретаря", "дилема самаритянина", "дилема стрілочника" та інші. Пандемія COVID-19 породила низку моральних дилем. Наприклад, дослідження *Everett et al.* (*2021*) представлене в Nature Human Behavior, вивчає – чи повинні лідери віддавати перевагу власним громадянам над людьми в інших країнах під час розподілу обмежених ресурсів.

Про дилеми люди зазвичай вважають за краще не замислюватися. А у тих, хто розмірковує, гіпотетичний вибір може і не збігтися з реальним, якщо виникне справжня дилема. Але саме перед такими дилемами ставлять гібридні зловмисники звичайних непідготовлених громадян. Пошук виходу з ситуації, яка не має хороших рішень вимагає **внутрішньої роботи людини із собою**.

Рішення "нерозв'язних" дилем потребує не лише певного когнітивного рівня, але й розвинутого морального мислення. Моральні міркування людини розвиваються протягом всього її життя. І так само, як і когнітивні – вони можуть бути здобуті під час навчання. Визнання та знання того, як керувати етичними та моральними дилемами, можна вважати **етичною навичкою**.

Багатообіцяючим способом навчити приймати рішення в умовах дилем є створення **спільного ігрового середовища**, у якому відбувається симуляція складної ситуації і люди співпрацюють для її вирішення через прийняття рішень. В іграх з дилемами гравці занурюються у сценарій, який базується на гострій, всеосяжній, неоднозначній проблемі, яку не вийде класифікувати як одновимірну чи суто технічну. Гра в дилему дозволяє змоделювати будову (структуру) ситуаційної обізнаності під час кризи та напрацювати навички контролю над складною ситуацією в міру її розвитку, що є однією з найскладніших частин в урегулюванні кризи.

Ситуаційна обізнаність (situation awareness, SA) – це сприйняття елементів навколишнього середовища в обсязі часу і простору, розуміння її значення і прогнозування їх стану в найближчому майбутньому (*Endsley, 1995; c. 36*)

Підтримувати точну спільну операційну картину та досягти спільної ситуаційної обізнаності значно складніше, ніж отримати індивідуальну ситуаційну обізнаність. Отже, формат командної гри є ефективним і з точки зору тренування навичок співпраці та взаємодії.

Розробка ігри-дилеми – не проста навчальна задача. Тут може стати у нагоді **досвід** дослідницької організації **TNO** (https://www.tno.nl/en/), яка, серед інших завдань, вивчає та запроваджує комплексні освітні підходи для набуття компетентності у прийнятті складних рішень. Низка проєктів, в яких спеціалісти TNO взяли участь, спрямовані на конструювання навчального процесу через ігри-дилеми. Результатом проєкту "GATE3 Pilot Safety" (Нідерланди, 2009–2012 рр.) стала "Гра мерів", The Mayor Game (*Stubbé et al., 2014*). Вона вчить приймати політичні рішення на високому рівні і використовується для того, щоб навчити нових мерів управлінню кризовими ситуаціями. Більшість мерів Нідерландів пройшли навчання за сценаріями цієї гри. Підхід узагальнено у потужному консорціумі більш ніж 30-ти команд в рамках проєкту DRIVER+ (https://www.driver-project.eu/).

При конструюванні ігор-дилем, TNO спирається на ідею **експериментального навчання**. Згідно з нею, учасники повинні активно розвивати свої навички, щоб самостійно набути тактичних знань і вмінь. Навчання має відбуватись на досвіді. Принципи, які підтримують цю ідею, мають бути дотримані у дизайні ігри-дилеми:

– "спочатку практика – потім теорія": теоретичний зміст не надається заздалегідь, а здобувається під час вирішення реалістичних проблем; окрім того, що досвід робить людей сприйнятливими до теорії, це одночасно тренує розв’язання проблем в абсолютно нових ситуаціях;

– "рефлексія обов’язкова" – набутий досвід необхідно концептуалізувати та закріпити після кожного сценарію; цей процес об’єднує знання та успішні стратегії застосування цих знань, які є типовими компетентностями експерта.

– "короткий цикл" – що дозволяє швидко повторювати короткі вправи і зіткнутися з якомога більшою кількістю різних налаштувань протягом визначеного часу (тренування має відбуватись не довше одного дня).

– "поступове збільшення складності" – замість одного великого сценарію слід програти серію сценаріїв, складність яких поступово зростає.

– "виклик": навчальні проблеми мають бути досить складними, щоб кинути виклик, бо навчання важким шляхом – це найшвидший шлях до кваліфікації.

– "тренування частини завдання": гра має бути спрямована лише на прийняття рішень і відділена від процедурного контексту.

Дизайн гри з дилемою зазвичай складається з елементів, представлених у **табл. 5**.

Таблиця 5. Складові ігри-дилеми

Складова	**Характеристика**
1	**2**
Проблема	Має бути всеосяжною, неоднозначною, не одновимірною і не технічною, складною (складатися з багатьох дилем) і вимагати прийняття стратегічного рішення. Приклади "поганих проблем", які підходять для гри в дилеми: – (потенційний) зовнішній конфлікт (наприклад, гібридна війна); – великомасштабне лихо або природна криза (наприклад, пандемія); – геополітична та економічна конкуренція (наприклад, Арктика); – внутрішня дестабілізація або поляризація (наприклад, тероризм)
Роль (Актор)	Можуть грати багато гравців (часто – у командах з двох осіб, щоб стимулювати взаємне обговорення). Усім гравцям призначається одна роль, яка є фіксованою для всієї гри. Актор та його повноваження пов›язані з проблемою. Наприклад, у разі конфлікту між країнами актором можна вибрати генерального секретаря НАТО, а якщо країну може дестабілізувати терористичний акт, актором можна вибрати прем'єр-міністра країни

Продовження Таблиці 5

1	2
Дилеми	Дилеми мають задовольняти таким вимогам: – двійковість – повинні мати лише два варіанти відповіді: "так" чи "ні"; – реальність – варіанти (так чи ні) повинні мати недоліки (подвійне зв’язування); – реалістичність для цільової групи: багато рішень, які ми вважаємо дилемами, для практиків є безглуздими, потрібно це перевірити; – незалежність – кожна дилема має бути незалежною у серії дилем, не впливати на загальний хід сценарію, щоб уникнути зайвої деталізації. Приклади дилем в умовах гібридних загроз: – пріоритетність (стимулювання бізнесу vs. соціальне забезпечення); – короткотермінові ефекти та довгострокові наслідки; – зіткнення інтересів (прибутки vs. безпека у справі Huawei); – моральні проблеми (пожертвувати селом для порятунку міста); – юридичні проблеми (конфіденційність vs. безпека проти злочинів); – відоме проти невідомого (поточна чи принципово нова технологія); – індивідуальні інтереси проти спільних (фінансова криза ЄС); – протистояння чи пом›якшення наслідків (викриття vs. дипломатія); – дія проти роздумів (швидко реагування COVID-19 vs. вичікувати); – зміна проти стабільності та безперервності (наприклад, Brexit); – прагматичне проти ідеологічного (китайські інвестиції vs. Неприйняття порушення прав людини в Китаї)
Передісторія	Пояснює поточну ситуацію та містить інформацію про: – відповідних акторів (державні та недержавні);

Продовження Таблиці 5

1	**2**
	– кілька важливих подій (минулих, поточних, запланованих); – географічне та часопросторове середовище; – деякі виклики, з якими доводиться стикатися акторам. Має бути обмеженою 1 сторінкою. Зайві деталі не потрібні, лише магістральні лінії. Гравці можуть самостійно додати вмісту з фактичної ситуації. Брифінг краще представити колективно, з деякими ілюстраціями
Дорадчі ролі	Радники надають аргументи, щоб мотивувати "так" чи "ні" рішення. Визначають до 10 радників і обирають для кожної дилеми відповідних. Поради (кількість радників) для кожної дилеми мають бути збалансовані: мають бути порадники, які кажуть "так", і порадники, які кажуть "ні", бажано майже у рівній кількості. Але якщо є один дійсно вагомий аргумент, можна вирішити, щоб інші радники заперечували цей аргумент, і таким чином створили баланс у якості замість кількості. Кожна порада має ґрунтуватися на 1 або 2 переконливих аргументах. Поради слід формулювати дуже стисло; не варто згадувати всі деталі і бути дипломатичними. Краще – чорно-білі точні поради замість сірих. Радники мають представляти всі інтереси, думки та/або організації. При визначенні радників рекомендується вибирати різні рівні. Наприклад, усі – на рівні політики, або всі на рівні міністра тощо. Дорадчі ролі, які часто використовуються та змішуються в іграх: – національні департаменти (економічні, закордонні справи, МО); – національні агентства (розвідка, охорони здоров’я); – міжнародні організації (НАТО, ЄС, ВООЗ); – глави держав; – генеральні директори великого бізнесу тощо

Co-funded by the
Erasmus+ Programme
of the European Union

Продовження Таблиці 5

1	**2**
Зворотній зв'язок	Для деяких ігор можна надавати заздалегідь приготовлені відгуки про прийняті рішення. Це необов›язково. Такі відгуки мають форму журнальної статті. Вони містять опис того, що сталось, якщо прийнято рішення "так" (або – що сталось при рішенні "на") та забезпечать перехід до наступних подій
Рефлексія	Основна дискусія відбувається після гри в дилему. Модератор дозволяє всім запропонувати свій вибір і, що важливо, свою мотивацію та аргументи. Обговорення займає 30-45 хвилин. Зручно використовувати інструменти підтримки, такі як система електронного голосування, яка забезпечує швидкий огляд відмінностей у відповідях. Це також полегшує анонімну реєстрацію результатів, що може бути корисним для виявлення спільних тем під час багаторазової гри в дилему. Журнал також є корисним для оцінки дилем. Іноді здається, що дилема не є справжньою, що може відображатися в одностайних балах

Фахівцями TNO були розроблені **рекомендації для конструювання** ігор-дилем, які не обмежують формат ігри (можна відтворювати у паперовому форматі та у програмній версії), а також не висувають особливих вимог до ведучого (достатньо обмеженого навчання).

Але рекомендації містять такі обмеження:

– ігри слід запускати на дуже короткий проміжок часу – до 90 хвилин (включно з обговоренням);

– гравці мають отримуватимуть поради щодо будь-якої дилеми, зазвичай це 4–5 різних порад з різних точок зору;

– кожна гра складається з набору у 6–8 дилем.

Перш ніж використовувати гру в дилеми у реальній аудиторії, рекомендується провести попереднє тестування: переглянути

всі дилеми та консультативні аргументи (бажано експертами), за необхідності – доопрацювати чи перефразувати їх; а також – перевірити час, необхідний для повної гри.

Також важливо врахувати, що гра має на мети надати навички прийняття рішень у прискореному режимі. Тому не бажано, щоб учні витрачали час на ознайомлення з інструментами такої гри. Отже, важливою вимогою до конструювання гри-дилеми є зручність використання. Особи, які приймають стратегічні рішення, мають використовувати гру без навчання та, бажано, без пояснень – гра повинна мати простий інтуїтивно-зрозумілий інтерфейс.

Приклад розробки та результати тестування гри-дилеми "Dilemma: Flooding game" ("Гра у повінь") презентовані у звіті *DRIVER+ project (2017), p.22–32*, більше прикладів тестування з описом різних реалістичних сценаріїв дилем – на офіційному сайті проєкту у розділі Trials (https://www.driver-project.eu/trials/).

Джерела посилань

Dilemma. Oxford Reference. Available at: https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095718683

Endsley, M. R. (1995). Measurement of Situation Awareness in Dynamic Systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37 (1), 65–84. doi: https://doi.org/10.1518/001872095779049499

Everett, J. A. C., Colombatto, C., Awad, E., Boggio, P., Bos, B., Brady, W. J. et al. (2021). Moral dilemmas and trust in leaders during a global health crisis. Nature Human Behaviour, 5 (8), 1074–1088. doi: https://doi.org/10.1038/s41562-021-01156-y

França, J. B. S., Borges, M. R. S. (2020). Systematizing the impacts projection of complex decisions in work groups. SN Applied Sciences, 2 (7). doi: https://doi.org/10.1007/s42452-020-3086-4

Method and Tool for Training Decision-Making Context -D934.12 (2017). DRIVER+ project. Available at: https://www.driver-project.eu/wp-content/uploads/2018/02/DRIVER-_D934.12_Method-and-tool-for-training-decision-making-context.pdf

Stubbé, H., Ven, J. G. M., van de Hrehovcsik, M. (2014). Games for top civil servants: An integrated approach. Cases on the Societal Effects of Persuasive Games. IGI Global, 32–50. doi: https://doi.org/10.4018/978-1-4666-6206-3.ch003

8. НАВЧАННЯ СТІЙКОСТІ

Марія Головянко[1]
Світлана Гришко[1]
[1]Харківський національний університет радіоелектроніки

8.1. Формування стійкості до переконання: теорія щеплення

Існує хибна думка, що дискусія навколо проблемного питання сама по собі приносить користь. Думка є хибною, бо часто суперечка лише зміцнює учасників у власній думці та в цінностях.

Викладання дисциплін з протидії гібридним загрозам має враховувати **соціальну теорію щеплення**, згідно якої власні переконання чи ставлення стають більш стійкими під впливом "ослаблених" контраргументів (*Compton, 2013*).

Слабкі контраргументи викликають опір в адресата, що дозволяє йому зберегти свої переконання перед обличчям майбутньої, сильнішої атаки. Після впливу **слабких контраргументів** (наприклад, які були поєднані зі спростуваннями), одержувач буде шукати підтверджуючу інформацію, щоб **ще більше посилити свою позицію**. Через це ставлення чи переконання стають стійкими до сильнішої атаки.

Соціальна теорія щеплення (теорія інокуляції) була розроблена за аналогією з медичною теорією формування імунітету через щеплення (**табл. 8**).

Ідея **вакцини від промивання мізків** ("vaccine for brainwash") передбачає наступне: замість того, щоб бомбардувати людей підтверджуючими фактами (аргументами), слід завчасно надати "ослаблену" дозу переконливого маніпулятивного контраргументу.

Таблиця 6. Теорія щеплення: порівняння біологічної та соціальної вакцинації

Елементи імунного захисту	**Біологічне середовище**	**Соціальне середовище**
1	**2**	**3**
Науковий бекграунд	Імунологія (*Луї Пастер, 19 ст.*)	Теорія інокуляції (*McGuire, 1961*)
Об'єкт захисту	Живі організми	Переконання та ставлення людей
Загроза (чужорідний агент)	Інфекційний агент (патоген): молекули інших організмів, мікробні клітини, пошкоджені клітини власного організму	Нав'язані маніпулятивні контраргументи , що призводять до маніпулятивних зрушень у переконаннях і думках людей
Імунітет – здатність до опору чужорідним агентам	Здатність живого організму чинити опір інфекції	Здатність людей зберігати свої переконання та ставлення в умовах маніпулятивних впливів
Імунна система – сукупність елементів організму, які захищають його від чужорідних агентів. Функції: розпізнавання загрози, вироблення відповіді (протидії), нейтралізація загрози, запам'ятовування загрози та відповіді	Складається із сукупності органів, тканин, клітин. Ключові функції виконують лімфоцити: – Т-клітини – розпізнання "свій – чужий"; – В-клітини – вироблення антитіл;– фагоцити, NK-клітини – захоплення та знищення бактерій та вірусів	Складається із сукупності когнітивних процесів. Ключові функції виконують аргументи та контраргументи: (і) адресат піддається контраргументам, які "вибивають" його із зони комфорту; (іі) запускається процес пошуку аргументів для підтвердження своїх переконань та спростування контраргументів

Продовження Таблиці 6

1	2	3
Відповідь імунної системи	Антитіла – білкові сполуки, що виробляються організмом для нейтралізації чужорідних агентів	Аргументи – обґрунтування (доводи, інформація) для підтвердження своїх переконань
Імунна пам'ять – прискорена та посилена специфічна відповідь на повторну взаємодію з чужорідним агентом. Формується як здатність "запам›ятати": 1) кожного чужорідного агента, 2) свою унікальну відповідь	Принцип роботи: Т- та В-лімфоцити утворюються з первинною імунною відповіддю і продовжують циркулювати з кров'ю як носії клітини пам'яті. При вторинній відповіді ці клітини розмножуються, збільшуючи потрібні лімфоцити	Принцип роботи: Аргументи, знайдені під час первинного зіткнення з контраргументами, зміцнюють власні переконання. Це готує мислення до опору наступним, переконливішим повідомленням
Щеплення (імунізація) – створення штучного імунітету	Введення збудника хвороби в здоровий організм. Щеплення має бути досить сильним, щоб спровокувати вироблення антитіл, але не настільки, щоб викликати важку інфекцію	"Вприскування" контраргументів в інформаційне поле. Контраргументи мають бути досить сильними, щоб породити бажання вступити в полеміку, але не настільки сильними, щоб змінити власну думку людини
Вакцина	Штучно створений препарат, що складається з ослаблених збудників хвороб	Штучно розроблені слабкі контраргументи, які легко спростувати

Його спростування ("prebunk") дозволить надати психологічний опір майбутнім переконливим інформаційним атакам.

Багатообіцяючим засобом для щеплення виявились ігри через їх потенційну розважальну цінність та обсяг добровільного сприйняття, а також рівень когнітивних зусиль, необхідних для їх виконання (*Roozenbeek & Van der Linden, 2021*).

Можна рекомендувати використання з метою щеплення проти дезінформації онлайн ігри на основі вибору, в яких **студенти беруть на себе роль зловмисника**:

– браузерна онлайн-гра **Bad News / погані новини** (www.getbadnews.com) для боротьби з дезінформацією, створена DROG та Кембриджським університетом, у якій гравці беруть на себе роль виробника фейкових новин;

– українська версія гри-щеплення для протидії фейковим новинам – онлайн-гра "**Маніпулятор**" (https://texty.org.ua/d/manipulator-game/) створена незалежним виданням TEXTY.ORG.UA у співпраці з Інститутом масової інформації (IMI), де так само гравці беруть на себе роль виробника фейкових новин, але вже в українському контексті;

– он-лайн гра **Harmony Square / Площа Гармонії** (www.harmonysquare.game), розроблена DROG, Глобальним центром взаємодії Державного департаменту США та Кембриджським університетом) бореться не лише з дезінформацією, але й з поляризацією суспільства; гравці беруть на себе роль "Головного спеціаліста з дезінформації" для зловмисної організації, їм доручено організувати кампанію впливу, щоб роз'єднати людей на площі Гармонії;

– онлайн-гра **Go Viral! / Ставай вірусним!** (www.goviralgame.com), розроблена DROG, Кембриджським університетом та Кабінетом Міністрів Великобританії) зосереджується на дезінформації про COVID-19;

– онлайн-гра **Cranky Uncle / Вередливий дядько** (www.crankyuncle.com), розроблена Джоном Куком з Університету Monash у співпраці з креативним агентством Autonomy) зосереджена на кліматичній дезінформації. Цікаво те, що Cranky Uncle розроблено для використання у навчальному процесі, а на веб-сайті є посібник для викладача, який пояснює застосування гри як навчального інструменту;

– онлайн-гра **ДемоГратія** (https://www.demogratia.platfor.ma), яка розроблена на основі курсу з громадянської освіти "Демократія: від теорії до практики", створеного Міжнародною фундацією виборчих систем (IFES) в Україні для закладів вищої освіти. Тут пропонується набір життєвих ситуацій, які вимагають застосування на практиці методів громадянської участі. Гра пропонує гравцю спробувати себе у різних ролях та в таких ситуаціях, де (як і в реальності) не існує правильних відповідей.

Також можна зробити важливі методичні висновки з практики застосування теорії інокуляції у навчальному процесі:

– надаючи приклади ворожих наративів, потрібно пам'ятати, що це – патогени або контраргументи (табл.8), які обов›язково мають бути спростовані. Не слід сподіватись, що студенти впораються самостійно. Більш того, потрібна ретельна підготовка до спростування (до процедури "prebunk") та пошуку відповідних джерел та алгоритмів. Якщо така робота не підготовлена – краще утриматись від подібних прикладів, бо вони можуть перетворитись з "щеплення" на "хворобу", тобто привести до переконань, вигідних маніпулятору;

– поступовий перехід від легкого матеріалу до складного – дуже важливий. Це означає, що трудомістка робота з пошуку аргументації та створення багатошарових висновків, яка застосовується без попередньої підготовки студентів, може мати зворотній ефект. Складні конструкції критичного мислення виглядають менш привабливо ніж прості та зрозумілі "наративи-фастфуди", створені маніпуляторами. Важливо розпочати з простих аргументів та завдань, поступово переходячи до більш складних та неоднозначних моделей.

Більш глибоке застосування теорії щеплення пропонується як фундамент нової техніки навчання – інтелектуальний спаринг.

8.2. Методика інтелектуального спарингу

Системи штучного інтелекту і люди приймають рішення по-різному, проте вони вразливі до гібридних загроз (*Terziyan et al., 2018*). Одним з підходів до створення механізмів захисту від спроб нападника зірвати процес прийняття рішень є зіграти на схожостях

реакцій штучних та природних систем на гібридні атаки. Ідея полягає в тому, щоб провести паралелі між біологічними процесами, що відбуваються у голові людини, яка обирає одну з можливих альтернатив у точці прийняття рішень, і машинною логікою вибору вірного рішення (*Kaikova et al., 2022*).

Певні механізми, відпрацьовані у природі, довели свою ефективність, а значить, є ймовірність успіху у випадку запозичення їх для нових завдань у цифровому світі.

Розуміння цього підштовхує вчених до пошуку відповідей на безпекові запитання паралельно у когнітивних, суспільних та комп'ютерних науках, а також запозичення успішних результатів однієї галузі в інших. Так, фахівці із кіберзахисту копіюють біологічні процеси і механізми, розробляючи системи штучного інтелекту.

Для того, щоб створити свого роду "когнітивний імунітет" у людей, які приймають рішення, копіюється загальний механізм цифрового імунітету (зокрема, і цифрову вакцинацію), що використовується для систем штучного інтелекту із машинним навчанням (AI/ML) (*Branytskyi et al., 2022*). Вакцинація відбувається за допомогою змагального тренування. Її ефективність підтверджується теорією інокуляції, яка пояснює, як ставлення до складних проблем та людські переконання можна зробити більш стійкими до різноманітних викликів.

Теорія когнітивної інокуляції заснована за аналогію, розглянутою вище біологічною імунізацією та соціальним щепленням. Вона полягає у тому, що процес введення ослабленої дози вірусу для активації вироблення антитіл (щоб допомогти надати стійкість організму до майбутньої інфекції) можна аналогічним чином застосувати до контексту обробки інформації. Іншими словами, шляхом попередження людей та атакування їх суттєво послабленими дозами поведінкових викликів, стає можливим підняти рівень когнітивного опору або згенерувати "ментальні антитіла" проти майбутніх спроб переконання, частково через зміцнення структури мереж асоціативної пам›яті (*Compton, 2005*).

Предмет тренування треба шукати у когнітивно вразливих областях простору прийняття рішень: важливо обирати такі питання (професійні, соціальні, політичні тощо), де суспільство ще не має

єдиної (спільної) думки, а можливі варіанти рішень розбивають спільноту майже навпіл (50/50).

Приклад набору проблем-дилем, що використовується як стимул для змагальної підготовки (станом на 2021 рік), представлений в *Kaikova et al., 2022*. Зокрема такі набори дилем можна використовувати для вимірювання когнітивного статусу людини та його динаміки до, під час та після змагальної підготовки.

Кожен, кому пропонуються ці питання, повинен виконати когнітивну самооцінку, тобто оцінити особисту важливість кожного питання (у відсотках) та надати власну відповідь (рішення) на кожне питання, зазначаючи ступінь власної впевненості (відсоток для рішення "ТАК" проти відсотка для рішення "НІ"). Оптимальний набір питань для змагальної підготовки складається з дилем, які ділять студентів на рівні підмножини за відповідями.

Інтелектуальний спаринг – це змагальне тренування у вигляді інтелектуального бою у класі, який проводиться у формі диспуту між трьома групами студентів разом з викладачами (команда "Атакуючі", команда "Захисник" і команда "Арбітр", як показано на рис. 4, взаємозв'язок між якими копіює ідею архітектури змагальних нейронних мереж (GAN або Generative Adversarial Networks) (*Terziyan et al., 2021*).

Відомо, що диспут часто зміцнює учасників у їхніх власних думках і цінностях, тому тренування, подібне до диспутів, використовується для підвищення стійкості (resilience and robustness) цінностей та мислення учасників.

Команда «Нападник» винаходить запит "Дилема" для Захисника. Дилема вимагає відповіді (вибір із двох варіантів) і має багатоаспектну природу, що розділяє спільноту майже навпіл. Мета нападника насправді не неправильний вибір, а скоріше плутанина та максимальна (близько п'ятдесят на п'ятдесят) розбіжність всередині команди Defender. Тобто, чим більше розбіжностей, тим кращі результати нападника.

Команда «Захисник» повинна відповісти на "Дилему" вибором однієї спільної відповіді (керівник групи робить вибір з урахуванням аргументованого індивідуального вибору членів команди), зазначивши ступінь впевненості (залежно від результату

голосування). Перед цим кожен член команди (кожен відповідає за певний аспект проблеми) ділиться аргументами на користі власного вибору із командою. Мета захисника – зробити правильний вибір (з точки зору Арбітра) з високою впевненістю; тобто чим більше впевненості у правильності вибору, тим краще виступає Захисник.

Команда «Арбітр» має найвідповідальнішу роль надання зворотного зв'язку, іншими словами, реагування по кожній ітерації процесу на дії двох інших команд (нападників та захисників), підкріплюючи реакцію конкретними аргументами. Зворотній зв›язок містить числову оцінку якості запиту зловмисника та якості відповіді від Захисника з детальними коментарями. Очікується, що відгук у такому форматі допоможе покращити продуктивність обох команд-конкурентів на наступних ітераціях процесу. Тобто арбітр фактично є фасилітатором навчального процесу.

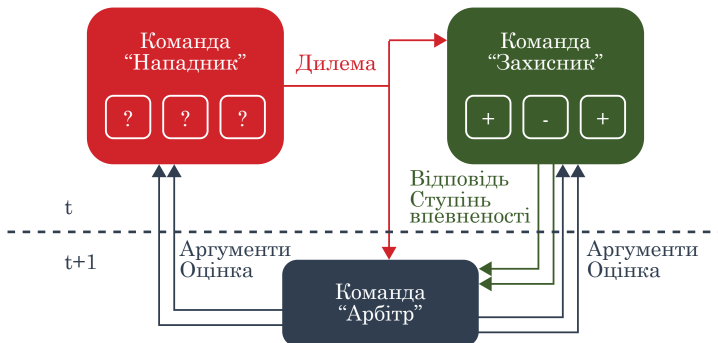


Рис. 3. Схема інтелектуального тренінгу, що моделює процеси в архітектурі Generative Adversarial Networks: одночасне навчання трьох команд студентів "Нападник", "Захисник" та "Арбітр" під час диспутів (*Kaikova et al., 2022*)

Передбачається, що під час тренувального процесу кожен студент хоча б один раз зіграє у кожній із трьох команд ("Атакуючий", "Захисник" і "Арбітр").

Ідеальний інструктор (викладач) такого спарингу має бути не стільки "двигуном" чи "провідником" змагального процесу навчання (або когнітивної вакцинації), скільки "каталізатором" цього процесу. При цьому бажано мати такі три якості:

– пристрасть (включаючи ентузіазм і натхнення);
– імпровізація (включаючи винахідливість і творчість;
– толерантність (у тому числі скромність і самокритичність).

Такі тренінги спрямовані на потребу суспільства, наприклад, українського, знайти "академічну вакцину" (WARN-вакцину) для підняття свідомості громадян та їхнього імунітету проти гібридних загроз, зокрема, когнітивного хакерства.

Зміст курсів WARN по суті слугує профілактичною вакциною, здатною зміцнити імунітет студентів від гібридних атак (як внутрішніх, так і зовнішніх) на їхню свідомість, совість, відповідальність, культуру та систему цінностей. Найважливішим академічним нововведенням є наступне:

Мета інтелектуального спарингу – це не оновлення особистих знань, навичок, переконань чи цінностей, а формування навичок для забезпечення надійності та стійкості переконань чи цінностей при створенні умов для їх розвитку

Тому новий підхід до інтелектуального спарингу (змагальної підготовки WARN) так само відрізняється від зомбування студентів новим змістом, наскільки процес вакцинації відрізняється від процесу отруєння. Студентами таких курсів є різні майбутні, знання та навички яких мають бути не тільки повними, але й надійними, щоб служити важливим фактором для сталого суспільства зі стійкими політичними, бізнесовими та виробничими процесами.

Джерела посилань

Branytskyi, V., Golovianko, M., Gryshko, S., Malyk, D., Terziyan, V., Tuunanen, T. (2022). Digital clones and digital immunity:

adversarial training handles both. International Journal of Simulation and Process Modelling, 18 (2), 124–139. doi: https://doi.org/10.1504/ijspm.2022.126106

Compton, J.; Dillard, J. P., Shen, L. (Eds.) (2013). Inoculation theory. The SAGE handbook of persuasion: Developments in theory and practice. Sage Publications, Inc., 220–236. doi: https://doi.org/10.4135/9781452218410.n14

Compton, J. A., Pfau, M. (2005). Inoculation Theory of Resistance to Influence at Maturity: Recent Progress In Theory Development and Application and Suggestions for Future Research. Annals of the International Communication Association, 29 (1), 97–146. doi: https://doi.org/10.1080/23808985.2005.11679045

Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., Titova, L. (2022). Hybrid Threats against Industry 4.0: Adversarial Training of Resilience. E3S Web of Conferences, 353, 03004. doi: https://doi.org/10.1051/e3sconf/202235303004

Roozenbeek, J., Van der Linden, S. (2021). Inoculation Theory and Misinformation. Riga: NATO Strategic Communications Centre of Excellence, 21. Available at: https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217

Terziyan, V., Golovianko, M., Gryshko, S.; Dimitrov, K. (Ed.) (2018). Industry 4.0 intelligence under attack: From cognitive hack to data poisoning. Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures. IOS Press, 110–125. doi: https://doi.org/10.3233/978-1-61499-888-4-110

Terziyan, V., Gryshko, S., Golovianko, M. (2021). Taxonomy of generative adversarial networks for digital immunity of Industry 4.0 systems. Procedia Computer Science, 180, 676–685. doi: https://doi.org/10.1016/j.procs.2021.01.290

ДОДАТОК А. ГЛОСАРІЙ ВАРГЕЙМІНГУ

Глосарій складено за матеріалами:

Cancian, M., Cancian, M., Heginbotham E. (2023). The First Battle of the Next War. Wargaming a Chinese Invasion of Taiwan. A Report of the CSIS International Security Program. CSIS, 165. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/230109_Cancian_FirstBattle_NextWar.pdf

The Development, Concepts and Doctrine Centre (2017). Wargaming Handbook. DCDC. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

№	Англійська термінологія	Українська термінологія
1	**Adjudication** is the act of determining the outcome of player decisions	**Винесення судового рішення** це акт визначення результату рішень гравців
2	**After action review** A facilitated discussion that actively involves the training audience	**Огляд після дії** Спрощена дискусія, яка активно залучає навчальну аудиторію
3	**Base case** The most likely assumption about each individual variable	**Основний варіант** Найбільш ймовірне припущення щодо кожної окремої змінної
4	**Base scenario** The scenario in which all assumptions are set to the base case	**Базовий сценарій** Сценарій, у якому всі припущення налаштовані на базові значення

№	Англійська термінологія	Українська термінологія
5	**Black** Colour used to represent organized and transnational organized criminals	**Чорний** Колір, який використовується для представлення транснаціональних організованих злочинців
6	**Blue** Colour used to represent friendly or allied forces	**Блакитний** Колір, який використовується для представлення дружніх або союзних сил
7	**Brown** Colour used to represent neutral actors or civilian population	**Коричневий** Колір, який використовується для представлення нейтральних акторів або цивільного населення
8	**Campaign analysis** A method involving the use of a model and techniques for managing uncertainty to answer questions about military operations	**Аналіз кампаній** Метод, що передбачає використання моделі та методів управління невизначеністю для отримання відповідей про військові операції
9	**Constructive simulation** Simulated people using simulated systems	**Конструктивне моделювання** Моделювання людської поведінки за допомогою симуляторів
10	**Descriptive data** Data on the occurrences of a given iteration, for example, who won and how many missiles were fired	**Описові дані** Дані про явища певної ітерації, наприклад, хто виграв і скільки ракет було випущено
11	**Event** An inserted major occurrence or a sequence of related incidents which fit into an exercise framework and are supported by incidents and injections designed to generate response(s) from the exercise participants	**Подія** Головне явище чи послідовність пов’язаних інцидентів, які вписуються у структуру навчань і підтримуються інцидентами, призначеними для генерування відповіді(й) від учасників навчань

№	Англійська термінологія	Українська термінологія
12	**Excursion case** Any alternate assumption wherein one or more of the variables is set to be different than the base case	**Нестандартний варіант** Будь-яке альтернативне припущення, в якому одна або більше змінних встановлені як відмінне від базового значення
13	**Excursion scenario** Any scenario wherein one or more variables are set to an excursion case	**Нестандартний сценарій** Будь-який сценарій, у якому для однієї або кількох змінних встановлено нестандартне значення
14	**Incident** An element or subset of an event. It is an action or situation that provides greater clarity to an event by using injections to bring an incident to the attention of the exercise participants for whom it was created	**Інцидент** Елемент або підмножина події. Це дія або ситуація, яка забезпечує більшу ясність події за допомогою вливань, щоб привернути увагу учасників до події, для яких вона була створена
15	**Iteration** One specific play through of the game under any scenario	**Ітерація** Одне конкретне проходження гри за будь-яким сценарієм
16	**Game** The overall project rather than a particular iteration or play-through	**Гра** Загальний проект, а не окрема ітерація чи проходження
17	**Green** Colour used to represent indigenous security forces	**Зелений** Колір, який використовується для представлення місцевих сил безпеки
18	**Live simulation** Real people using real systems	**Симуляція в реальному часі** Реальні люди, які використовують реальні системи
19	**Model** A mathematical or otherwise logically rigorous representation of a system or a system's behavior	**Модель** Математичне чи інше логічно точне представлення системи або поведінки системи

№	Англійська термінологія	Українська термінологія
20	**Net assessment** The comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations	**Чиста оцінка** Порівняльний аналіз військових, технологічних, політичних, економічних та інших факторів, що визначають відносну військову спроможність націй
21	**Operations research** The analytical study of military problems undertaken to provide a scientific basis for decision on action to improve military operations	**Дослідження операцій** Аналітичне дослідження військових проблем, яке проводиться з метою забезпечення наукової основи для прийняття рішень щодо дій з покращення військових операцій
22	**Setting** A geographic and strategic situation designed to provide all the conditions required to support the achievement of high level exercise aims and objectives. It can be real world, fictionalised or synthetic, is the framework on which the scenario can be developed	**Установки** Географічне та стратегічне положення, призначене для забезпечення всіх умов, необхідних для підтримки високого рівня гри. Це може бути реальний світ, вигаданий або синтетичний, це основа, на якій можна розробити сценарій
23	**Simulation** A method for implementing a model over time	**Симуляція** Метод реалізації моделі в часі
24	**Structured judgment** Any analysis that lays out assumptions in a logical, evidence-based argument that leads to a clear conclusion	**Структуроване судження** аналіз, який викладає припущення в логічну, засновану на доказах аргументацію, що веде до чіткого висновку
25	**Scenario** 1. A set of assumptions about each variable that provides the basis for playing one iteration of the game.	**Сценарій** 1. Набір припущень щодо кожної змінної, який забезпечує основу для однієї ітерації гри.

№	Англійська термінологія	Українська термінологія
	2. The background story that describes the historical, political, military, economic, cultural, humanitarian and legal events and circumstances that have led to the specific current exercise crisis or conflict. The scenario is designed to support exercise and training objectives and, like the setting, can be real, fictionalised or synthetic as is appropriate	2. Передісторія, яка описує історичні, політичні, військові, економічні, культурні, гуманітарні та правові події та обставини, які призвели до конкретної поточної кризи чи конфлікту у навчанні. Сценарій розроблений для підтримки цілей тренувань і тренувань і, як і обстановка, може бути реальним, вигаданим або синтетичним, залежно від обставин
26	**Systems analysis** The process of studying a procedure or business to identify its goal and purposes and create systems and procedures that will efficiently achieve them	**Системний аналіз** Процес вивчення процедури або діяльності, щоб визначити їх мету, задачі та створити системи і процедури, які ефективно їх досягнуть
27	**Unstructured judgment** Any analysis that lacks evidence, logical structure, or transparency	**Неструктуроване судження** Будь-який аналіз, якому бракує доказів, логічної структури чи прозорості
28	**Variable** A condition likely to have an impact on the analysis about which the project team must make an informed assumption	**Змінна** Умова, яка може вплинути на аналіз, щодо якої команда повинна зробити обґрунтоване припущення
29	**Wargaming** A simulation, by whatever means, of military operations involving two or more opposing forces, using rules, data, and procedures designed to depict an actual or assumed real life situation	**Варгеймінг** Симуляція військових дій будь-якими засобами за участю двох чи більше протиборчих сил з використанням правил, даних і процедур, призначених для відтворення фактичної чи припущеної реальної життєвої ситуації

Co-funded by the
Erasmus+ Programme
of the European Union

WARN

ДОДАТОК Б. ПРИКЛАД ОРГАНІЗАЦІЇ ВАРГЕЙМІНГУ ДЛЯ СПЕЦІАЛЬНОСТІ «ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ»

Михайло Білоконь[1]
[1]Харківський національний університет імені В. Н. Каразіна

Об'єднано декілька методів навчання: **метод кейс-стаді** (розбір конкретних ситуацій); **метод ділової гри** (моделювання конкретних можливих ситуацій, що відносяться до предмету навчання); інтегровано варгеймінг через **змагальні методи** – моделювання гібридного впливу, засноване на сценаріях в яких результат і послідовність подій впливають на рішення, що приймаються гравцями.

1 етап. Ознайомлення здобувачів із методами інформаційного впливу та тактиками поширення фейків (такими як клік-бейти, упереджена подача інформації, вигадані новини, etc.), та із порадами щодо відповідального споживання інформації.

2 етап. Розділення здобувачів на чотири групи (публічні службовці, представники громадянського суспільства, представники ЗМІ та група гібридного впливу "Червоні"). Ознайомлення здобувачів із заздалегідь підготовленими кейсами (описом наближеної до реальності ситуації, та роллю яку кожна група має виконувати).

3 етап. Відбувається моделювання "консультацій із громадськістю". Кожна група діє відповідно до своєї ролі: "Публічні службовці" проводять консультацію, самостійно організуючи процес; "Представники громадянського суспільства" представляють свою позицію щодо питань, визначених у кейсах; "Група впливу", використовуючи методи спотворення інформації, намагається реалізувати або просування потрібного їм наративу, або внести дестабілізацію у процес комунікації громадськості та публічної влади;

"ЗМІ" незалежно висвітлюють процес, роблять нотатки, та намагаються незалежно оцінити роботу інших груп.

Дії кожної групи відбуваються по черзі. Цей процес мають організовувати "публічні службовці".

4 етап. "Публічні службовці" приймають певне обґрунтоване рішення за підсумками 3 етапу. "ЗМІ" готують коментар щодо цього рішення.

5 етап. Рефлексія щодо заняття, під час якої здобувачі опрацьовують здобуті знання, навички, та розуміння інформаційного впливу та гібридних загроз у процесі комунікації громадськості та публічної влади.

Наукова публікація

**Едуард Балашов, Михайло Білоконь,
Тетяна Борозенцева, Марія Головянко, Світлана Гришко,
Тарас Жовтенко, Оксана Карпенко, Ольга Копієвська,
Олександр Котуков, Павло Худ**

МЕТОДИКА НАВЧАННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Посібник

ТОВ "ТЕХНОЛОГІЧНИЙ ЦЕНТР ГРУП"
вул. Шатилова дача, 4, м. Харків, Україна, 61165
Свідоцтво про внесення суб'єкта видавничої справи
No. 7582 від 01.02.2022
Опубліковано 26.10.2023 р.